

THEORETICAL ASPECTS OF THE  
BEHAVIOR OF DIGITAL CIRCUITS  
UNDER RANDOM INPUTS

S. K. KUMAR

DIGITAL INTEGRATED SYSTEMS CENTER REPORT  
DISC/81-3

DEPARTMENT OF ELECTRICAL ENGINEERING—SYSTEMS  
UNIVERSITY OF SOUTHERN CALIFORNIA  
LOS ANGELES, CALIFORNIA 90007

SEPTEMBER 1981

This work was supported in part by the National Science Foundation under Grant MSC-7826153 and the DOD under a VHSIC Phase 3 Contract No. DAAK20-80-C-0278 administered by the Department of the Army, Fort Monmouth, New Jersey.

FOREWARD TO DISC REPORT NO. 81-3

This report consists of the Ph.D. dissertation of Sarangan Krishna Kumar. The report presents several important new results dealing with the analysis of the behavior of digital circuits under random inputs. The results constitute a major contribution to the theory of random testing. A fundamental and new characterization of the probability function associated with a Boolean switching function is presented, as well as an extension of the concept of Boolean difference into the domain of random inputs. Both single and multiple operating points are considered.

Melvin A. Breuer  
Professor  
University of Southern California  
8 September 1981



## ACKNOWLEDGEMENTS

I would like to express my deepest sense of appreciation to Professor Melvin A. Breuer for his encouragement during the course of this thesis. I consider it my privilege to have worked with him. His scholarship has been a constant source of inspiration and his constructive comments have helped tremendously in the presentation of this thesis. My sincere thanks go to Professors John Hayes and Alan Schumitzky for being on my committee.

I take this opportunity to thank my parents and my sister Nalini for their moral support and encouragement during my graduate education in this country. My heartfelt thanks go to my many friends including Ramesh Babu, Ayee Goundan, Malathi Iyengar, Suresh Iyengar, Anita Rau, Kewal Saluja, T. Sridhar and Ray Turner for their help during the course of this thesis.

My special thanks to Kris Pendleton for a super job in typing the final manuscript.

## ABSTRACT

This dissertation deals with the analysis of the behavior of digital circuits under probabilistic (or random) inputs.

A new algorithm for computing a probability expression  $F(X_1, X_2, \dots, X_n) = \Pr(f=1)$  of a Boolean function  $f(x_1, x_2, \dots, x_n)$  being one, as a function of input probabilities  $X_1, X_2, \dots, X_n$  is presented.  $F$  is characterized by a spectrum vector  $S$ . A matrix  $P$  with the property  $S = AP$  where  $A$  is the minterm vector of the function  $f$  is introduced. The relationship between  $S$ , and both the Reed-Muller canonic (RMC) coefficient vector  $a$  and the Walsh coefficient vector  $C$  of a Boolean function  $f$  is discussed.

The partial differential of  $F$  with respect to the variable  $X_i$ ,  $\frac{\partial F}{\partial X_i}$  is introduced. The relationship between the Boolean Difference of a function  $f$  with respect to  $x_i$ ,  $\frac{df}{dx_i}$  and  $\frac{\partial F}{\partial X_i}$  is developed. Deterministic test generation procedures based on  $\frac{\partial F}{\partial X_i}$  are presented. The average probability of detection over a set of faults is used as the objective function in generating "optimal" random tests. Experimental results are presented to gain insight into the problem of random test generation. The analysis is

extended to intermittent faults.

A matrix model for the analysis of synchronous sequential circuits under probabilistic inputs is developed. The criteria for probabilistic synchronization (the final state is independent of the initial state) is shown to be related to the spectral radius of the matrix. The rate of convergence to the final state is also discussed. A method to analyze the probability of detecting single stuck-at-0 (1) faults in synchronous sequential circuits is then presented.

The concept of multiple operating point random testing is introduced. It is shown that using multiple operating points leads to more effective testing.

A class of input probability distributions with the property that no two  $n$ -variable combinational functions have the same output probability under these distributions is identified.

## TABLE OF CONTENTS

	page
ACKNOWLEDGEMENTS .....	ii
ABSTRACT .....	iii
LIST OF FIGURES .....	viii
LIST OF TABLES .....	xv
CHAPTER 1 INTRODUCTION .....	1
1.1 Previous Work and Problem Definition .....	1
1.2 Thesis Outline .....	4
CHAPTER 2 PROBABILISTIC ASPECTS OF BOOLEAN SWITCHING FUNCTIONS VIA A TRANSFORM TECHNIQUE .....	6
2.1 Introduction .....	6
2.2 Probability Expression Analysis .....	7
2.2.1 Mathematical Background .....	8
2.2.2 Properties of Probability Expressions and Probability Functions .....	10
2.3 Transform Techniques .....	19
2.3.1 Matrix Technique to Compute the Spectrum S .....	19
2.3.2 Computational Complexity Analysis .....	25
2.3.3 Properties of the Matrix P .....	27
2.3.4 Realizability of Boolean Functions .....	31
2.3.5 Properties of Spectrum S .....	34
2.4 RMC Expansion and Probability Transform .....	40
2.4.1 Introduction .....	40
2.4.2 Relationship Between the Spectrum S and RMC Coefficients of a Boolean Function f .....	41



	page
2.4.3 Minimization of RMC Expansion .....	49
2.4.3.1 Procedure to Generate the Minimal RMC Form .....	52
2.4.3.2 Complexity Analysis .....	55
2.5 Walsh Transform and Probability Transform .....	56
2.5.1 Relation Between the Spectrum S and the Walsh Coefficients of a Boolean Function F .....	59
2.5.2 Computational Complexity .....	63
2.6 Probability Transform Domain Analysis of Boolean Functions .....	63
2.6.1 Mapping Between Boolean Functions .....	63
2.6.2 Analysis of Properties of Boolean Functions .....	69
2.7 Concluding Remarks .....	74
CHAPTER 3 TEST GENERATION FOR COMBINATIONAL CIRCUITS .....	76
3.1 Introduction .....	76
3.2 Probability Expressions and Differential Calculus .....	80
3.3 Deterministic Test Generation .....	84
3.4 Random Test Generation .....	102
3.5 Intermittent Failure Analysis .....	133
3.5.1 Introduction .....	133
3.5.2 Intermittent Fault Model .....	134
3.6 Concluding Remarks .....	140
CHAPTER 4 PROBABILISTIC ASPECTS OF SYNCHRON- OUS SEQUENTIAL CIRCUITS .....	141
4.1 Introduction .....	141
4.2 Model for Analysis of Synchronous Sequential Circuits under Random Inputs .....	143
4.3 Probabilistic Synchronization .....	155
4.4 Analysis of Synchronous Sequential Circuits under Faulty Conditions ....	172

	page
4.4.1 Fault Model .....	173
4.4.2 Procedure to Determine the Probability of Detecting a Fault .....	174
4.5 Conclusions .....	177
CHAPTER 5 MULTIPLE OPERATING POINT RANDOM TESTING OF COMBINATIONAL CIRCUITS .....	179
5.1 Introduction .....	179
5.2 Functions Used in Multiple Operating Point Random Testing .....	180
5.3 Theory of Multiple Operating Point Random Testing .....	186
5.4 A Special Class of Input Prob- ability Distributions .....	198
5.5 Concluding Remarks .....	207
CHAPTER 6 CONCLUDING REMARKS .....	210
REFERENCES .....	213
APPENDIX REED-MULLER FORM OF SEQUENTIAL CIRCUITS .....	218

# LIST OF FIGURES

Figure		page
2.1	A circuit realizing the function $f = x_1x_2 \vee x_2x_3$ .....	11
2.2	Truth table for the function $f = x_1x_2 \vee \bar{x}_2x_3$ .....	25
2.3	Reed Muller canonic realization of a Boolean function $f$ .....	42
2.4	Vector A for $f = \bar{x}_1x_3 \vee x_2x_3 \vee x_1\bar{x}_2\bar{x}_3$ .....	48
2.5	Walsh matrix of order 8 .....	57
2.6	Function $f$ and its spectrum $S$ .....	64
2.7	Interchange of variables $x_k$ and $x_\ell$ .....	66
2.8	Spectrum $S, S'$ for the functions $f$ and $\bar{f}$ .....	66
2.9	Complementation of variable $x_K$ .....	68
3.1	A method for testing digital circuits using pseudo-random patterns .....	79
3.2	Circuit of Example 3.3 .....	89
3.3	Circuit of Examples 3.4 and 3.11 .....	93
3.4	Circuit of Examples 3.5, 3.6, and 3.10 .....	97
3.5	Summary of relationships developed in Sections 3.2, 3.3, and 3.4.1 .....	114
3.6	Variation of $\beta = p \cdot PD_{avg}(N)$ with respect to variables $X_3$ and $X_4$ .....	123
3.7	Relationship between $K$ , the number of faults, and the probability that the expected number of faults detected equals $K$ , for different $N$ , for the circuit of Example 3.11 .....	125
3.8	Relationship between $K$ , the number of faults, and $\Omega_1(K)$ for different $N$ for the circuit of Example 3.11 .....	126

Figure	page
3.9 Relationship between $K$ , the number of faults, and $\Omega_2(K)$ for different $N$ for the circuit of Example 3.11 .....	127
3.10 [Maximum $p \cdot PD_{avg}(N) - p \cdot PD_{avg}(N)$   uniform distribution ] as a function of $N$ .....	129
3.11 Circuit of Example 3.12 .....	130
3.12 Intermittent fault model .....	135
3.13 Model for intermittent fault $f_{I_1}$ .....	136
3.14 Model for intermittent fault $f_{I_0}$ .....	136
3.15 Circuit without the intermittent fault for Example 3.12 .....	137
3.16 Modified circuit including the effect of intermittent fault $f_{I_1}$ for Example 3.12 .....	137
4.1 Synchronous sequential circuit using D flip-flops .....	144
4.2 State table for a sequential circuit .....	156
4.3 Synchronizing tree for the sequential circuit of Figure 4.2 .....	156
4.4 Relationship between $A$ and $S(C,A)$ for the circuit of Example 4.6 .....	171
5.1 Circuit of Example 5.1 .....	182
5.2 Circuit of Example 5.2 .....	188
5.3 Circuit of Example 5.3 .....	194



# LIST OF TABLES

Table		page
2.1	Spectrum of Boolean Functions of Two Variables .....	32
2.2	Gray Codewords and Corresponding Polarity Function of 3 Variables .....	52
3.1	Table Showing All Possible Values for $\frac{\partial F}{\partial X_i}$ , $X_j \in \{0,1\}$ .....	84
3.2	Table Showing the Output Signal Vaues in Terms of the Input Signal Values and the Expression $\frac{\partial F}{\partial X_i}$ .....	95
3.3	Table Showing Input Distributions Corresponding to Maximum, Minimum $p \cdot PD_{avg}$ and $p \cdot PD_{avg}$ Corresponding to Uniform Distribution for Circuit of Example 3.11 .....	119
3.4	Number of Input Distributions and Associated $p \cdot PD_{avg}$ for Circuit of Example 3.11 .....	121
3.5	Table Showing the Result of the Variable Metric Method for the Circuit of Example 3.11 .....	122
3.6	Table Showing Various Input Probability Distributions and the Associated $p \cdot PD_{avg}$ for Circuit of Example 3.12 .....	131
3.7	Number of Input Distributions and Associated $[p \cdot PD_{avg}]$ for Circuit of Example 3.12 ...	132
4.1	Minterm Vectors $A_{B(\underline{y}^+;i)}$ , $i = 1,2,3,4$ .....	149
5.1	Optimal and Worst Case Distributions Corresponding to Maximum $p \cdot PD_{avg}$ and Minimum $p \cdot PD_{avg}$ for $N = 2,4,6,8$ under $OP^{(1)}$ for	

Table	page
Example 5.3 .....	195
5.2 Number of Input Distributions and Associated $\lfloor p \cdot PD_{avg}(N) \rfloor$ for $N=2,4,6,8$ under $OP^{(1)}$ .....	195
5.3 Optimal Worst Case Distributions for $N=2,4,6,8$ under $OP^{(2)}$ .....	196
5.4 Number of Input Distributions and the Associated $\lfloor p \cdot PD_{avg} \rfloor$ under $OP^{(2)}$ .....	196
5.5 Output Probabilities of 16 Functions of 2 Variables .....	200
5.6 Output Probabilities of the 16 Functions of Variables Under $P(3,2)$ .....	206
5.7 Output Probabilities of the 16 Functions of 2 Variables Under $P(4,2)$ .....	208

## CHAPTER 1

### INTRODUCTION

#### 1.1 Previous Work and Problem Definition

Fault diagnosis is concerned with the detection and location of hardware faults in digital circuits.

Testing digital circuits consists of applying a sequence of input patterns to a circuit under test, measuring the response at the outputs, and comparing it with a precomputed normal response. In the absence of any discrepancy between the observed and expected response the circuit "passes" the test and is said to function correctly. Otherwise, the circuit is said to contain a physical fault.

Physical faults are often modeled as logical faults.

For a combinational circuit which realizes the function  $f(x_1, x_2, \dots, x_n)$ , a logical fault  $\alpha$  changes the function realized to  $f_\alpha(x_1, x_2, \dots, x_n)$ . The stuck-line fault model is one such logical fault model. In this model it is assumed that all faults of interest in a circuit can be represented by gate input and output lines that are stuck-at logical value 0 (s-a-0) or stuck-at logical value 1 (s-a-1).

Many algorithms have been presented for test generation in digital circuits. These algorithms can be divided

into two classes which will be referred to as deterministic and random test generation techniques. Algorithms such as the Boolean Difference [SHB68] and the D-algorithm [Ro66] are examples of the first class.

Random test generation algorithms employ pseudo-random patterns to test a circuit. In one method, a test pattern sequence of length  $L$  is applied to a known good circuit and to the circuit under test. The output responses are compared and the circuit is considered to be fault free if no discrepancy is observed in the output responses. In another method, a preconstructed randomly generated test sequence is usually processed through a mini-computer and applied to the circuit under test. The expected response and a fault dictionary are determined by a prior simulation using a software model of the circuit under test.

Several studies have been presented to analyze the "goodness" of random input patterns in testing a circuit [Ra71, AA72, HB73, AA75a, AA75b, SM75, SM76, DB76]. The expected number of faults detected as a function of the number of input patterns applied is presented in [HB73] for a class of NAND circuits. The probability of sensitizing the longest path in a NAND tree network is discussed in [AA75a]. Based upon this analytical measure, the number of random patterns needed to achieve a desired probability



of sensitizing the longest path in a NAND tree network can be computed. The problem of determining the optimal input probabilities for generating "effective" input patterns for a NAND tree network is presented in [AA76].

The error latency of a fault is the number of input patterns applied to a circuit, while the fault is present, until the first incorrect output vector due to the fault is observed [SM75]. Based upon this concept, the "goodness" of a random input pattern set can be determined. Another analytical measure deals with the number of random input patterns required to achieve a desired probability of detecting the "hardest" fault to detect under equiprobable inputs [DB76]. The determination of the probability that a random input will drive the output of a combinational circuit is discussed in [PM75a].

Some work dealing with the theoretical aspects of the testing of sequential circuits under random inputs has been carried out in [SM76,Lo77]. The concept of error latency in sequential circuits is discussed in [SM76]. Quantitative measures for the efficiency of compact testing of sequential circuits under random inputs is presented in [Lo77].

Little effort has been devoted to the theoretical aspects of the behavior of digital circuits under random inputs. We therefore propose to investigate the behavior of combinational and sequential circuits under random

inputs.

## 1.2 Thesis Outline

This thesis is an investigation of the behavior of digital circuits under random inputs.

In Chapter 2 we deal with the generation of a probability expression  $F(X_1, X_2, \dots, X_n) = \Pr(f=1)$  of a Boolean function  $f(x_1, x_2, \dots, x_n)$  being one, as a function of the input probabilities  $X_1, X_2, \dots, X_n$ . It is established that there exists a matrix  $P$  with the property that the spectrum  $S$  (an equivalent representation for  $F$ ) is given by the relationship  $S = AP$  where  $A$  is the minterm vector of the function  $f$ . The structure of  $P$  is useful in establishing useful properties of  $S$  (and  $F$ ). In addition, the relationship between  $S$ , and both the Reed Muller Canonic (RMC) coefficient vector  $a$  and the Walsh coefficient vector  $C$  are established.

In Chapter 3 we deal with the issue of testing in digital circuits. Various relationships between  $\frac{df}{dx_i}$ , the Boolean difference of a function  $f$  with respect to a variable  $x_i$  and  $\frac{\partial F}{\partial X_i}$ , the partial differential of the function  $F = \Pr(f=1)$  with respect to the variable  $X_i = \Pr(x_i=1)$  are established. It is also shown that the expressions for  $\frac{\partial F}{\partial X_i}$  can be used in deterministic and random test generation algorithms. Experimental results for "optimal" ran-

dom test generation are presented. The main objective is to provide insight into test generation.

Chapter 4 deals with the analysis of the behavior of synchronous sequential circuits under random inputs. A matrix model is constructed for this purpose. Synchronization aspects based on the properties of the matrix model are presented. In addition, a model for the analysis of faulty circuits is presented. Using this model, the probability of detecting a fault can be determined.

In Chapter 5 we discuss the concept of multiple operating point random testing. The objective is to gain insight into the problem of improving the "effectiveness" of using random patterns in testing a circuit. Finally, a class of input probability distributions, with the special property that no two  $n$ -variable combinational functions have the same output probability, is presented.

## CHAPTER 2

### PROBABILISTIC ASPECTS OF BOOLEAN SWITCHING FUNCTIONS VIA A TRANSFORM TECHNIQUE

#### 2.1 Introduction

Several transform techniques which map a Boolean function into various domains have been extensively studied, such as the Reed Muller canonic (RMC) representation and the Walsh coefficient representation C. An extensive treatment of many transform techniques for discrete functions is presented in [DDT78]. These transforms have been used in fault diagnosis [BH78, Ma77], in the classification of Boolean functions [De65, Ed75, Le71] and in logic design [Ed75, Hu73, Hu77, EH78, Le71, MH78].

There has been considerable interest in the area of random testing of digital circuits [Ra71, Br71, AA75, SLC75, SM75, SM76, PM75a, PM75b]. The probability expression  $F(X_1, X_2, \dots, X_n)$  of a Boolean function  $f(x_1, x_2, \dots, x_n)$  can be used to compute the probability that  $f$  equals 1 given a set of values for  $X_i$ , the probability that  $x_i$  equals 1, for  $i = 1, 2, \dots, n$ . The probability expression is a key factor in generating efficient random tests for digital circuits.

The main contribution in this chapter deals with the generation of  $F$ . We have identified and constructed a



highly structured matrix  $P$  with the property that the spectrum  $S$  (an equivalent representation for  $F$ ) is given by  $S = AP$  where  $A$  is the minterm vector of the function  $f$ . The elegant structure of  $P$  is helpful in identifying useful properties of  $P$ ,  $S$  and  $F$ .

We have also discovered several relations between the spectrum vector  $S$ , the RMC coefficient vector  $a$ , and the Walsh coefficient vector  $C$  of the Boolean function  $f$ . It has been established in this chapter that the RMC coefficient vector  $a$  can be obtained trivially from the spectrum vector  $S$ . The reverse transformation is computationally harder.

In Section 2.2 we discuss the background material and the properties of the probability expressions of Boolean functions. In Section 2.3 we present the transform matrix  $P$  used in constructing  $S$ . Properties of the matrix  $P$  and the spectrum  $S$  are analyzed. In Sections 2.4 and 2.5 the relationships between the spectrum  $S$  and the RMC and Walsh transform coefficients are presented. Properties of Boolean functions in the spectrum domain are analyzed in Section 2.6.

## 2.2 Probability Expression Analysis

In this section we present the basic material required for the development of subsequent sections and some fundamental properties of probability expressions of Boolean functions.

### 2.2.1 Mathematical Background

Logic signals in digital circuits will be denoted by the symbols  $x_1, x_2, \dots$ , etc. Boolean functions will be denoted by  $f, f_1, f_2, \dots$ , etc.

Definition 2.1: The probability of a logic signal  $x_1$  expressed as  $X_1 = \Pr(x_1=1)$  is a real number over the closed interval  $[0,1]$  and denotes the probability of the logic signal  $x_1$  being 1.

Definition 2.2: The probability that a logic signal  $x_1$  equals 0 is given by

$$\Pr(x_1=0) = 1 - \Pr(x_1=1) = 1 - X_1 .$$

Definition 2.3: The probability function  $F^*$  of a Boolean function  $f(x_1, x_2, \dots, x_n)$  is a mapping given by

$$F^* : [\Pr(x_1=1), \Pr(x_2=1), \dots, \Pr(x_n=1)] \rightarrow \Pr(f=1) .$$

We will refer to an expression for the probability function as the probability expression  $F(X_1, X_2, \dots, X_n)$ . We shall use the terms probability expressions and probability functions interchangeably except when there is a need to distinguish between them. The following lemmas establish the relationship between Boolean operations on logic signals and the corresponding operations on probabilities of logic

signals.

Lemma 2.1 [PM75a]: The Boolean AND of two independent signals  $x_1, x_2$  in the Boolean function  $f = x_1 x_2$  corresponds to a probability expression  $F = X_1 X_2$  where  $F$  denotes the probability that  $f = 1$  and the implied operation is multiplication.

Lemma 2.2 [PM75a]: The Boolean OR of two independent signals  $x_1, x_2$  in the Boolean function  $f = x_1 \vee x_2$  corresponds to a probability expression

$$F = X_1 + X_2 - X_1 X_2 .$$

Lemma 2.3 [PM75a]: The Boolean AND of signal  $x_1$  with itself in the Boolean expression  $f = x_1 x_1$  corresponds to the probability expression  $F = X_1$ .

Parker and McCluskey [PM75a] devised two algorithms for deriving the output probability for a combinational logic circuit in terms of a set of input probabilities. Algorithm 1 suffers due to the need for canonical sum of products form (or the minterm form) for a Boolean function and Algorithm 2 suffers due to the need for circuit description and exponent suppression.<sup>1</sup> Exponents arise in the calculation of probability expressions when Lemmas 2.1-2.3

---

<sup>1</sup> Exponent suppression means that  $X_i^m$  can be replaced by  $X_i$ .

are used in the presence of signals with reconvergent fan-out. It has been shown informally in [PM75a] that when a probability expression for any Boolean function is calculated by treating all signals as though they are independent and exponents in the resulting expression suppressed, a correct probability expression results.

The following example illustrates this approach to calculating the probability expression.

Consider the circuit of Figure 2.1. Using Lemma 2.1 we have

$$\Pr(x_1 x_2 = 1) = X_1 X_2$$

$$\Pr(x_2 x_3 = 1) = X_2 X_3.$$

Using Lemma 2.2, ignoring the dependency between the two terms, we have

$$\Pr(x_1 x_2 \vee x_2 x_3 = 1) = X_1 X_2 + X_2 X_3 - X_1 X_2^2 X_3. \quad (2.1)$$

Exponent suppression yields the correct probability expression

$$F = X_1 X_2 + X_2 X_3 - X_1 X_2 X_3.$$

A formal proof for this approach is presented in [Ko77].

### 2.2.2 Properties of Probability Expressions and Probability Functions

Lemma 2.4: A probability expression for  $f = f_1 \vee f_2$  is given

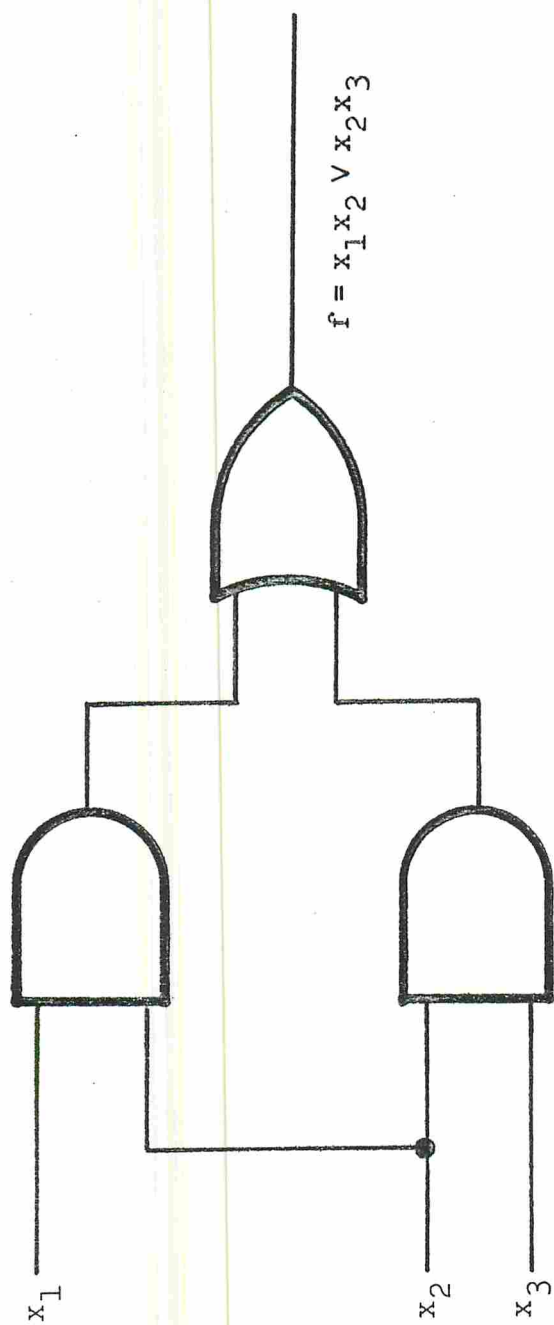


Figure 2.1. A circuit realizing the function  $f = x_1x_2 \vee x_2x_3$



by  $F = F_1 + F_2 - F_3$  where  $F_1, F_2$  are probability expressions for  $f_1, f_2$  and  $F_3$  is a probability expression for  $f_3 = f_1 \cdot f_2$ .

Proof: From probability theory we know that if A, B, and C are events such that if  $A = B \cup C$  then the probability of event A = probability of event B + probability of event C - (probability of event B and event C occurring together).

The result follows immediately. ■ ■

Lemma 2.4 can be applied repeatedly to obtain a probability expression for  $f = f_1 \vee f_2 \vee \dots \vee f_n$ .

We now present a procedure to compute an output probability expression of a general combinational circuit given any sum of product expression. No knowledge of circuit description is required and exponent suppression is avoided because exponents do not arise.

Procedure 2.1: Let  $f = p_1 \vee p_2 \vee \dots \vee p_n$  where  $p_i, i = 1, \dots, n$  are product terms.

1. Compute  $\text{Pr}(p_1=1)$  using Lemma 1.3.
2.  $i \leftarrow 2$
3. Do while  $i \leq n$
4. Compute  $\text{Pr}(p_1 \vee p_2 \vee \dots \vee p_i) = 1$  using Lemma 2.4 as follows:

$$\begin{aligned} \Pr((p_1 \vee p_2 \vee \dots \vee p_i) = 1) &= \Pr((p_1 \vee p_2 \vee \dots \vee p_{i-1}) = 1) \\ &+ \Pr(p_i = 1) \\ &- \Pr[(p_1 \vee p_2 \vee \dots \vee p_{i-1})(p_i) = 1]. \end{aligned}$$

5.  $i \leftarrow i+1$ .

6. End while.

Theorem 2.1: Procedure 2.1 yields an exponent-free probability expression for the function  $f$ .

Proof: By induction on  $n$ , the number of product terms.

1. Consider  $n=1$  and let  $p_1 = \tilde{x}_1 \tilde{x}_2 \dots \tilde{x}_k$  where  $\tilde{x}_i$  represents either the literal  $x_i$  or  $\bar{x}_i$ .

Since the logic signals  $x_1, x_2, \dots, x_k$  are independent, using Lemma 2.1, we have an exponent-free expansion for the probability expression of the product term  $p_1$ .

2. Consider  $n=2$

$$f = p_1 \vee p_2.$$

Then

$$\begin{aligned} \Pr(p_1 \vee p_2 = 1) &= \Pr(p_1 = 1) + \Pr(p_2 = 1) \\ &- \Pr(p_1 p_2 = 1). \end{aligned}$$

We know that the terms  $p_1$  and  $p_2$  have exponent-free probability expressions. The product term  $p_1 p_2 = p$  consists of independent variables. Hence the probability expression

has no exponent.

3. Assume true for any  $n$  product term function and prove for  $n+1$  terms

$$\begin{aligned} \Pr[p_1 \vee p_2 \vee \dots \vee p_{n+1}=1] &= \Pr[p_1 \vee p_2 \vee \dots \vee p_n=1] \\ &\quad + \Pr[p_{n+1}=1] \\ &\quad - \Pr[(p_1 \vee p_2 \vee \dots \vee p_n)(p_{n+1})=1]. \end{aligned}$$

The term  $\Pr[p_1 \vee p_2 \vee \dots \vee p_n=1]$  is exponent-free by assumption and the term  $\Pr[(p_1 \vee p_2 \vee \dots \vee p_n)(p_{n+1})=1]$  is really  $\Pr[p_1 p_{n+1} + p_2 p_{n+1} + \dots + p_n p_{n+1}=1]$ . It has  $n$  terms and is therefore exponent free. Thus Procedure 1 yields an exponent-free probability expression. ■ ■

Example 2.1: Consider the Boolean function  $f = x_1 x_2 \vee x_2 x_3$ . Applying Procedure 2.1 we have

$$\begin{aligned} 1. \quad \Pr(x_1 x_2=1) &= X_1 X_2 \\ 2. \quad \Pr(x_1 x_2 \vee x_2 x_3=1) &= \Pr(x_1 x_2=1) + \Pr(x_2 x_3=1) \\ &\quad - \Pr(x_1 x_2 \cdot x_2 x_3=1) \\ &= \Pr(x_1 x_2=1) + \Pr(x_2 x_3=1) \\ &\quad - \Pr(x_1 x_2 x_3=1) \\ &= X_1 X_2 + X_2 X_3 - X_1 X_2 X_3. \end{aligned} \tag{2.2}$$

Theorem 2.2: Every Boolean function  $f(x_1, x_2, \dots, x_n)$  has a unique probability function  $f^*$ .



Proof: It is obvious that for functions having  $2^n(0)$  min-terms, the probability function is 1(0). Consider the case where  $f$  has  $k$  minterms,  $0 < k < 2^n$ . Let minterm  $m_1$  be of the form  $\tilde{x}_1 \tilde{x}_2 \dots \tilde{x}_n$  where  $\tilde{x}_1 = x_1$  or  $\bar{x}_1$ . Setting the probability of all inputs corresponding to uncomplemented (complemented) variables to 1 (0) we have  $\Pr(m_1 = 1) = 1$ . Therefore, there exists at least one set of input probabilities for which  $F^* \neq 0$  for all nontrivial functions.

Let  $f_1, f_2$  be two nontrivial Boolean functions having the same probability function  $F^*$  and  $f_1 \neq f_2$ .

Using the concept of conditional probability [Pa69]

$$\begin{aligned} \Pr(f_1 \bar{f}_2 = 1) &= \Pr(f_1 = 1) \text{ AND } \Pr(f_2 = 0 / f_1 = 1) \\ &= 0. \end{aligned} \quad (2.3)$$

Similarly

$$\Pr(\bar{f}_1 f_2) = 0. \quad (2.4)$$

Combining equations (2.3) and (2.4)

$$\begin{aligned} \Pr[f_1 \oplus f_2 = 1] &= \Pr[\bar{f}_1 f_2 = 1] + \Pr[f_1 \bar{f}_2 = 1] \\ &= 0. \end{aligned}$$

But we know that  $f = 0$  is the only function with  $\Pr[f = 1] = 0$ . Hence  $f_1 \oplus f_2 = 0$  and  $f_1 = f_2$  contradicting our assumption. ■■

Corollary 2.1: The probability function  $F^*$  for a Boolean function  $f$  is unaltered in the presence of redundant product terms in the expression for  $f$ .

Example 2.2: Consider the Boolean function (expression)

$f_1 = x_1x_2 \vee x_2x_3 \vee x_1x_2x_3$  where the last term is redundant.

Applying Procedure 2.1 we have

$$1. \Pr(x_1x_2=1) = X_1X_2 \text{ and } \Pr(x_2x_3=1) = X_2X_3$$

$$\begin{aligned} 2. \Pr(x_1x_2 \vee x_2x_3 \vee x_1x_2x_3=1) &= \Pr(x_1x_2 \vee x_2x_3=1) \\ &\quad + \Pr(x_1x_2x_3=1) \\ &\quad - \Pr((x_1x_2 \vee x_2x_3)x_1x_2x_3=1) \\ &= X_1X_2 + X_2X_3 - X_1X_2X_3 \\ &\quad + \cancel{X_1X_2X_3} - \cancel{X_1X_2X_3} \end{aligned}$$

which is the same as expression (2.2).

Theorem 2.3:  $F(X_1, X_2, \dots, X_n) = f(x_1, x_2, \dots, x_n)$  where  $X_i = x_i \in \{0, 1\}$ .

Proof: Case 1:  $f(x_1, x_2, \dots, x_n) = 0$  for a given set of input values  $x_1^a, x_2^a, \dots, x_n^a$ .

$$\begin{aligned} F(X_1, X_2, \dots, X_n) &\Big|_{X_1=x_1^a, X_2=x_2^a, \dots, X_n=x_n^a} \\ &= \Pr(f=1) \Big|_{x_1=x_1^a, \dots, x_n=x_n^a} \\ &= 0. \end{aligned}$$

Case 2:  $f(x_1, x_2, \dots, x_n) = 1$  for a given set of input values  $x_1^b, x_2^b, \dots, x_n^b$ .

$$\begin{aligned}
& F(X_1, X_2, \dots, X_n) \Big|_{X_1=x_1^b, \dots, X_n=x_n^b} \\
&= \Pr(f=1) \Big|_{x_1=x_1^b, \dots, x_n=x_n^b} \\
&= 1.
\end{aligned}$$

■ ■

It can be seen that  $F$ , when evaluated over the domain of  $(0,1)^n$ , has the same (binary) value as  $f$  when evaluated for the same  $n$ -tuple.

Theorem 2.4: The function  $F(X_1, X_2, \dots, X_n)$  can be completely characterized by a vector  $S$  of the coefficients of the product terms  $1, X_1, X_2, \dots, X_n, X_1X_2, X_1X_3, \dots, X_{n-1}X_n, X_1X_2X_3, \dots, X_1X_2X_3X_4, \dots, X_1X_2X_3 \dots X_n$ .

Proof: Follows directly from Theorem 2.1.

■ ■

Definition 2.4: The row vector of  $B_{2n}$  of product terms is defined recursively as follows:

$$\begin{aligned}
B_1 &\stackrel{\Delta}{=} 1; \quad B_{2n-1} \stackrel{\Delta}{=} [b_0(X_1, X_2, \dots, X_{n-1}), b_1(X_1, X_2, \dots, X_{n-1}), \\
&\quad \dots, b_{2^{n-1}-1}(X_1, X_2, \dots, X_{n-1})].
\end{aligned}$$

Then

$$B_{2n} \stackrel{\Delta}{=} [b'_0, b'_1, \dots, b'_{2^n-1}]$$

where

$$a) \quad b'_i = b_i(X_1, X_2, \dots, X_{n-1}) \text{ with any occurrence of }$$

$X_j$  in  $b_i$  replaced by  $X_{j+1}$  in  $b'_i$  for  $i = 0, 1, \dots, 2^{n-1}-1$  and  $j = 1, 2, \dots, n-1$ ; and

$$b) \quad b'_i = X_1 b'_{i-2^{n-1}} \text{ for } i = 2^{n-1}, 2^{n-1}+1, \dots, 2^n-1.$$

Example 2.3:  $B_2 = [1 \quad X_1]$ .

There are four terms in  $B_4$ . The first two terms in  $B_4$  are derived from the terms in  $B_2$  by replacing each variable  $X_j$  by  $X_{j+1}$ . Hence the first two entries in  $B_4$  are  $[1 \quad X_2]$ . The next two entries in  $B_4$  are derived from the first two entries of  $B_4$  by multiplying each entry by the variable  $X_1$ . Hence

$$B_4 = [1 \quad X_2 \quad X_1 \quad X_1 X_2].$$

Similarly

$$B_8 = [1 \quad X_3 \quad X_2 \quad X_2 X_3 \quad X_1 \quad X_1 X_3 \quad X_1 X_2 \quad X_1 X_2 X_3].$$

We note that  $B_{2^n}$  contains all the product terms required to characterize a function of  $n$  variables. The "ordering" scheme described is required for development of further results.

Consider a function of  $n$  variables. The corresponding probability expression  $F$  is given by

$$F = S_{b_0} b_0 + S_{b_1} b_1 + S_{b_2} b_2 + \dots + S_{b_{2^n-1}} b_{2^n-1}$$

and hence  $F = SB^T = S^T B$ . The row vector  $S$  of the coefficients is called the *spectrum*  $S$  of the Boolean function  $f$ .

From Theorem 2.2 and Definition 2.4, we have the following theorem.

Theorem 2.5: Every Boolean function  $f$  has a unique spectrum  $S$ . ■ ■

Example 2.4: Consider the Boolean function  $f = x_1x_2 \vee \bar{x}_2x_3$

$$\begin{aligned} F(X_1, X_2, X_3) &= X_1X_2 + (1-X_2)X_3 \\ &= X_1X_2 + X_3 - X_2X_3. \end{aligned}$$

Since  $B \stackrel{\Delta}{=} [1 \ X_3 \ X_2 \ X_2X_3 \ X_1 \ X_1X_3 \ X_1X_2 \ X_1X_2X_3]$  it follows that  $S = [0 \ 1 \ 0 \ -1 \ 0 \ 0 \ 1 \ 0]$ .

### 2.3 Transform Techniques

In this section we develop a matrix transform technique for computing the spectrum  $S$  of a Boolean function of  $n$  variables and equivalently the probability expression of the function.

#### 2.3.1 Matrix Technique to Compute the Spectrum $S$

Definition 2.5: Minterm vector  $A$  of a Boolean function  $f$  is defined as

$$A \stackrel{\Delta}{=} [A_0, A_1, \dots, A_i, \dots, A_{2^n-1}]$$

where

$A_i = 0$  (1) if and only if minterm  $m_i$  is absent (present) in  $f$

and

$m_i = \tilde{x}_1 \tilde{x}_2 \dots \tilde{x}_j \dots \tilde{x}_n$  where  $\tilde{x}_j = x_j$  ( $\bar{x}_j$ ) if and only if the corresponding component in the binary  $n$ -tuple representing integer  $i$  is 1 (0) for  $j = 1, 2, \dots, n$ .

Definition 2.6: Define a matrix  $P$  recursively as

$$P_{1 \times 1} = 1; \quad P_{2^n \times 2^n} \triangleq \left[ \begin{array}{c|c} P_{2^{n-1} \times 2^{n-1}} & -P_{2^{n-1} \times 2^{n-1}} \\ \hline 0 & P_{2^{n-1} \times 2^{n-1}} \end{array} \right].$$

Example 2.5:

$$P_{1 \times 1} \triangleq [1]$$

$$P_{2 \times 2} = \left[ \begin{array}{c|c} 1 & -1 \\ \hline 0 & 1 \end{array} \right]$$

$$P_{4 \times 4} = \left[ \begin{array}{cc|cc} 1 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ \hline 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{array} \right]$$

$$P_{8 \times 8} = \left[ \begin{array}{cccc|cccc} 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 0 & 1 & 0 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & -1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ \hline 0 & 0 & 0 & 0 & 1 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right].$$



It can be seen that the matrix  $P$  is upper triangular, the entries in the main diagonal are 1, and  $P$  has one eigenvalue equal to 1 and of multiplicity  $2^n$ .

Theorem 2.6: Let  $P_{2^n \times 2^n} \cdot B_{2^n}^T = [M_0, M_1, \dots, M_1, \dots, M_{2^n-1}]^T$ .

Then  $M_i$  is a probability expression for the minterm  $m_i$ ,  $i = 0, 1, \dots, 2^n-1$ .

Proof: By induction on  $n$ , the number of variables.

1. Consider  $n = 1$ .

Then

$$P_{2 \times 2} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

and

$$B_2 = [1 \quad X_1].$$

Hence

$$P_{2 \times 2} \cdot B_2^T = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ X_1 \end{bmatrix} = \begin{bmatrix} 1-X_1 \\ X_1 \end{bmatrix}.$$

We know that  $M_0 = 1-X_1$  is a probability expression for the minterm  $m_0 = \bar{x}_1$  and  $M_1 = X_1$  is a probability expression for the minterm  $m_1 = x_1$ .

2. Consider  $n = 2$ .

Then

$$P_{4 \times 4} = \begin{bmatrix} 1 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

and

$$B_4 = [1 \quad X_2 \quad X_1 \quad X_1 X_2].$$

Hence

$$P_{4 \times 4} \cdot B_4^T = \begin{bmatrix} 1 - X_2 - X_1 + X_1 X_2 \\ X_2 - X_1 X_2 \\ X_1 - X_1 X_2 \\ X_1 X_2 \end{bmatrix}.$$

The components of the resulting vector are probability expressions for minterms  $m_0, m_1, m_2$  and  $m_3$ .

3. Assume true for  $(n-1)$  variables and prove for  $n$  variables

$$P_{2^n \times 2^n} \cdot B_{2^n}^T = \left[ \begin{array}{c|c} P_{2^{n-1} \times 2^{n-1}} & -P_{2^{n-1} \times 2^{n-1}} \\ \hline 0 & P_{2^{n-1} \times 2^{n-1}} \end{array} \right] \left[ \begin{array}{c} B' \\ B'' \end{array} \right]$$

where  $B' = [b'_0, b'_1, \dots, b'_{2^{n-1}-1}]$  and  $B'' = [b'_{2^{n-1}}, b'_{2^{n-1}+1}, \dots, b'_{2^n-1}] = [X_1 b'_0, X_1 b'_1, \dots, X_1 b'_{2^{n-1}-1}]$ .

Note that row  $i$  of  $P_{2^{n-1} \times 2^{n-1}} \cdot B'$  is a probability



expression for minterm  $m_{i-1}$  over the variables  $x_2, x_3, \dots, x_n$ .

Consider row  $i$  of  $P_{2^n \times 2^n}$ ,  $1 \leq i \leq 2^{n-1}$ . Then

$$\begin{aligned} \sum_{j=1}^{2^n} p_{ij} b'_{j-1} &= \sum_{j=1}^{2^{n-1}} p_{ij} b'_{j-1} + \sum_{j=2^{n-1}+1}^{2^n} p_{ij} b'_{j-1} \\ &= \sum_{j=1}^{2^{n-1}} p_{ij} b'_{j-1} + \sum_{j=1}^{2^{n-1}} -x_1 p_{ij} b'_{j-1} \\ &= (1-x_1) \sum_{j=1}^{2^{n-1}} p_{ij} b'_{j-1}. \end{aligned} \quad (2.5)$$

But  $\sum_{j=1}^{2^{n-1}} p_{ij} b'_{j-1}$  is a probability expression for the term  $\tilde{x}_2 \dots \tilde{x}_n$ .

Hence, equation (2.5) represents a probability expression for the minterm  $\bar{x}_1 \tilde{x}_2 \tilde{x}_3 \dots \tilde{x}_n$ , that is, for minterm  $m_{i-1}$  of  $n$  variables.

Similarly for  $2^{n-1}+1 \leq k \leq 2^n$  we can show that

$$\sum_{j=1}^{2^n} p_{kj} b'_{j-1} = \sum_{j=2^{n-1}+1}^{2^n} p_{kj} x_1 b'_{j-(2^{n-1}+1)} \quad (2.6)$$

which is a probability expression for the minterm

$x_1 \tilde{x}_2 \tilde{x}_3 \dots \tilde{x}_n$ , that is, for minterm  $m_{k-1}$  of  $n$  variables. ■ ■

Corollary 2.2: Let

$$P_{2^n \times 2^n} \triangleq \begin{bmatrix} P_0 \\ P_1 \\ \vdots \\ P_i \\ \vdots \\ P_{2^n-1} \end{bmatrix}$$

where  $P_i$  is a row vector,  $i = 0, 1, \dots, 2^n - 1$ . Then  $P_i$  is the spectrum  $S$  of the minterm  $m_i$ . ■ ■

Theorem 2.7: Let  $A$  be the minterm vector for the function  $f(x_1, x_2, \dots, x_n)$ . Then

$$S = AP. \quad (2.7)$$

Proof: We know that the column vector  $PB^T$  consists of the probability expressions of the ordered minterms  $m_i$ ,  $i = 0, 1, \dots, 2^n - 1$ . For a given function  $f$ , a probability expression  $F$  is given by  $F = APB^T$ . Since  $F = SB^T$ , we have  $S = AP$ . ■ ■

Example 2.6: Figure 2.2 shows the truth table for the function  $f = x_1x_2 \vee \bar{x}_2x_3$ .

$$S = AP = [01000111] \begin{bmatrix} 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 0 & 1 & 0 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & -1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$x_1$	$x_2$	$x_3$	A
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Figure 2.2. Truth table for the function  
 $f = x_1x_2 \vee \bar{x}_2x_3$

$$S = [0 \ 1 \ 0 \ -1 \ 0 \ 0 \ 1 \ 0] .$$

Since

$$B_8 = [1 \ x_3 \ x_2 \ x_2x_3 \ x_1 \ x_1x_3 \ x_1x_2 \ x_1x_2x_3]$$

and

$$\begin{aligned} F &= SB^T \\ &= x_1x_2 + x_3 - x_2x_3 . \end{aligned}$$

### 2.3.2 Computational Complexity Analysis

Definition 2.7: A function  $g(n)$  is said to be  $\mathcal{O}(f(n))$  if there exists a constant  $c$  such that  $g(n) \leq cf(n)$  for all but some finite set of nonnegative values for  $n$ .

Computations of the form  $S = AP$  generally involve  $O(2^{2n})$  multiplications and additions where  $n$  is the number of Boolean variables in function  $f$ . However, the vector  $A$  contains elements taking values from the set  $\{0,1\}$  and therefore no multiplications are necessary. The following theorem, taking advantage of the recursive structure of the matrix  $P$ , offers a dramatic savings in computation.

Theorem 2.8: The computational complexity of  $S = AP$  is  $O(n2^n)$  additions.

Proof: We know that  $A = [A_0 A_1 \dots A_{2^{n-1}-1} A_{2^{n-1}} \dots A_{2^n-1}]$  and  $P$  is defined recursively as

$$P_{2^n \times 2^n} = \left[ \begin{array}{c|c} P_{2^{n-1} \times 2^{n-1}} & -P_{2^{n-1} \times 2^{n-1}} \\ \hline 0 & P_{2^{n-1} \times 2^{n-1}} \end{array} \right].$$

Let  $T[2^n]$  be the number of additions to be performed on a problem of size  $2^n$  [AHU74].

From the structure of  $P_{2^n \times 2^n}$  we see that in order to compute  $A \cdot P_{2^n \times 2^n}$  we need only to compute the following three subproblems:

- (1) compute  $[A_0 A_1 \dots A_{2^{n-1}-1}] \cdot P_{2^{n-1} \times 2^{n-1}}$ .
- (2) compute  $[A_{2^{n-1}} A_{2^{n-1}+1} \dots A_{2^n-1}] \cdot P_{2^{n-1} \times 2^{n-1}}$ .

(3) add  $2^{n-1}$  components corresponding to

$$[A_0 A_1 \dots A_{2^{n-1}-1}] \cdot P_{2^{n-1} \times 2^{n-1}} \\ + [A_{2^{n-1}} A_{2^{n-1}+1} \dots A_{2^n-1}] \cdot P_{2^{n-1} \times 2^{n-1}}.$$

The computation of the subproblems 1 and 2 is given by  $T[2^{n-1}]$ . Hence  $T[2^n] = 2T[2^{n-1}] + 2^{n-1}$ . By recursively expanding  $T[2^1]$  we have

$$\begin{aligned} T[2^n] &= 2[2T[2^{n-2}] + 2^{n-2}] + 2^{n-1} \\ &= 2^2 \cdot T[2^{n-2}] + 2 \cdot 2^{n-1} \\ &= 2^2 [2T[2^{n-3}] + 3 \cdot 2^{n-1}] \\ &\vdots \\ &= 2^{n-1} \cdot T[2] + (n-1)2^{n-1}. \end{aligned}$$

Since  $T[2] = 1$

$$T[2^n] = n \cdot 2^{n-1}.$$

Hence  $S$  can be computed in  $O(n \cdot 2^n)$  additions. ■ ■

### 2.3.3 Properties of the Matrix P

It is clear that  $p_{ij}$ , the  $(i,j)^{th}$  element of the matrix  $P$ , takes values from the set  $\{0, 1, -1\}$ .

Lemma 2.5: Consider  $P_{2^n \times 2^n}$ ,  $n = 1, 2, \dots$ . Then the

1. sum of the elements in the first column = 1
2. sum of the elements in column  $j = 0$ ,  $j = 2, 3, \dots, 2^n$



3. sum of the elements in row  $i = 0, i = 1, 2, \dots, 2^n - 1$
4. sum of the elements in the last row  $= 1$ .

Proof: We know by inspection that this is true for  $n = 1$  and  $n = 2$ . Assume true for  $n$  and prove for  $n+1$ . We know that

$$P_{2^{n+1} \times 2^{n+1}} = \left[ \begin{array}{c|c} P_{2^n \times 2^n} & -P_{2^n \times 2^n} \\ \hline 0 & P_{2^n \times 2^n} \end{array} \right].$$

1. Consider the sums

$$\sum_{i=1}^{2^{n+1}} p_{i1} = \sum_{i=1}^{2^n} p_{i1} + \sum_{i=2^{n+1}}^{2^{n+1}} p_{i1} = 1 + 0 = 1$$

$$\sum_{i=1}^{2^{n+1}} p_{ij} = \sum_{i=1}^{2^n} p_{ij} + \sum_{i=2^{n+1}}^{2^{n+1}} p_{ij} = 0 + 0$$

$$j = 2, \dots, 2^{n+1}.$$

2. Consider the row sums

$$\sum_{j=1}^{2^{n+1}} p_{ij} = \sum_{j=1}^{2^n} p_{ij} + \sum_{j=2^{n+1}}^{2^{n+1}} p_{ij} = 0 + 0$$

$$i = 1, 2, \dots, 2^n - 1$$

$$\sum_{j=1}^{2^{n+1}} p_{ij} = \sum_{j=1}^{2^n} p_{ij} + \sum_{j=2^{n+1}}^{2^{n+1}} p_{ij} = 1 - 1 = 0$$

$$i = 2^n$$

$$\sum_{j=1}^{2^{n+1}} p_{ij} = \sum_{j=1}^{2^n} p_{ij} + \sum_{j=2^{n+1}}^{2^{n+1}} p_{ij} = 0+0=0$$

$$i = 2^{n+1}, \dots, 2^{n+1}-1$$

$$\sum_{j=1}^{2^{n+1}} p_{ij} = \sum_{j=1}^{2^n} p_{ij} + \sum_{j=2^{n+1}}^{2^{n+1}} p_{ij} = 0+1=1$$

$$i = 2^{n+1}.$$

■ ■

Definition 2.8: Let  $M$  be an  $n \times n$  matrix. The inverse of  $M$ , denoted by  $M^{-1}$ , if it exists, is an  $n \times n$  matrix such that  $MM^{-1} = I$  where  $I$  is the unit matrix.

Theorem 2.9:  $P$  is invertible and  $P^{-1} = |P|$  where  $|P|$  represents the matrix whose elements are the absolute values of the elements of the matrix  $P$ .

Proof: By induction on  $n$ . We know  $P_{1 \times 1} \cdot |P|_{1 \times 1} = 1$

$$P_{2 \times 2} \cdot |P|_{2 \times 2} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Assume true for  $n$  and prove for  $n+1$ . Hence

$$P_{2^n \times 2^n}^{-1} = |P|_{2^n \times 2^n}$$

and recall that

$$P_{2n+1 \times 2n+1} = \left[ \begin{array}{c|c} P_{2n \times 2n} & -P_{2n \times 2n} \\ \hline 0 & P_{2n \times 2n} \end{array} \right].$$

Consider a matrix

$$M_{2n+1 \times 2n+1} = \left[ \begin{array}{c|c} |P|_{2n \times 2n} & |-P|_{2n \times 2n} \\ \hline 0 & |P|_{2n \times 2n} \end{array} \right]$$

$$P_{2n+1 \times 2n+1} M_{2n+1 \times 2n+1} = \left[ \begin{array}{c|c} P_{2n \times 2n} \cdot |P|_{2n \times 2n} & P_{2n \times 2n} \cdot |-P|_{2n \times 2n} \\ \hline 0 & 0 + P_{2n \times 2n} \cdot |P|_{2n \times 2n} \end{array} \right].$$

We know that  $|-P| = |P|$  for any  $n$ . Therefore

$$P_{2n+1 \times 2n+1} M_{2n+1 \times 2n+1} = \left[ \begin{array}{c|c} I & I-I \\ \hline 0 & I \end{array} \right] = I_{2n+1 \times 2n+1}$$

and

$$P_{2n+1 \times 2n+1}^{-1} = |P|_{2n+1 \times 2n+1}.$$

■ ■

Example 2.7: Consider

$$P_{4 \times 4} = \begin{bmatrix} 1 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Hence

$$P_{4 \times 4}^{-1} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

and

$$PP^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

#### 2.3.4 Realizability of Boolean Functions

In this section we attack the converse problem of finding the Boolean function corresponding to a given probability expression. The situation is complicated by the fact that not all expressions of the form

$$\begin{aligned} F(X_1, X_2, \dots, X_n) = & S_0 + S_{X_1} X_1 + \dots + S_{X_n} X_n + S_{X_1 X_2} X_1 X_2 + \dots \\ & + S_{X_1 X_2 \dots X_n} X_1 X_2 \dots X_n \end{aligned}$$

correspond to the probability expression of a Boolean function.

In Table 2.1 we list the spectrums for all Boolean switching functions of two variables.

Table 2.1. Spectrum of Boolean functions of two variables

Boolean Function $f$	$S_0$	$S_{x_2}$	$S_{x_1}$	$S_{x_1 x_2}$
0	0	0	0	0
1	1	0	0	0
$x_1$	0	0	1	0
$\overline{x_1}$	1	0	-1	0
$x_2$	0	1	0	0
$\overline{x_2}$	1	-1	0	0
$x_1 x_2$	0	0	0	1
$x_1 \vee x_2$	0	1	1	-1
$\overline{x_1 x_2}$	1	0	0	-1
$\overline{x_1} \vee x_2$	1	-1	-1	1
$\overline{x_1} \vee \overline{x_2}$	1	0	-1	1
$x_1 \vee \overline{x_2}$	1	-1	0	1
$x_1 \overline{x_2}$	0	0	1	-1
$\overline{x_1} x_2$	0	1	0	-1
$x_1 \oplus x_2$	0	1	1	-2
$\overline{x_1 \oplus x_2}$	1	-1	-1	2



Example 2.8: Consider  $F(X_1, X_2) = 1 - 2X_1 - 2X_2 + X_1X_2$ . The corresponding  $S = [1 \ -2 \ -2 \ 1]$ . From Table 2.1 we observe that none of the 16 Boolean functions of 2 variables has this spectrum and we conclude that  $F(X_1, X_2)$  does not correspond to any Boolean function.

Theorem 2.10:  $S$  corresponds to the spectrum of a Boolean function if  $SP^{-1} = A$  where  $A = [A_0 \ A_1 \ \dots \ A_{2^n-1}]$  and  $A_i \in \{0, 1\}$ ,  $i = 0, 1, \dots, 2^n-1$ .

Proof: We know that  $S = A \cdot P$  is the spectrum of a Boolean function if  $A$  is the minterm vector of the Boolean function. Since  $P$  is invertible,  $S$  is the spectrum of a Boolean function if  $A = A \cdot P \cdot P^{-1} = SP^{-1}$  is the minterm vector. ■ ■

Example 2.9: Consider the spectrum  $S = [1 \ -2 \ -2 \ 1]$  of Example 2.8

$$\begin{aligned} SP^{-1} &= [1 \ -2 \ -2 \ 1] \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \\ &= [1 \ -1 \ -1 \ -2] . \end{aligned}$$

Hence  $S$  is not realizable as a Boolean function.

### 2.3.5 Properties of Spectrum S

In this section we characterize some important properties of the spectrum S of Boolean functions.

Let  $(K; S^n)$  denote the  $K^{th}$  component of the spectrum of a Boolean function of n variables.

Theorem 2.11: Let  $N = \{1, 2, \dots, n\}$ . Then

$$S_0 \in \{0, 1\}$$

$$S_{X_1} \in \{0, \pm 1\} \quad \forall i \in N$$

$$S_{X_1 X_j} \in \{0, \pm 1, \pm 2\} \quad \forall i, j \in N \text{ and } i \neq j$$

$$\vdots$$

$$S_{X_1 X_2 \dots X_n} \in \{0, \pm 1, \pm 2, \dots, \pm 2^{n-1}\}.$$

Proof (by induction):

1. Consider  $n = 1$ ,  $P = [1]$ , and  $S = [S_0]$

$$S_0 = 0 \quad \text{if} \quad A = [A_0] = 0$$

and

$$S_0 = 1 \quad \text{if} \quad A = [A_0] = 1.$$

Hence

$$S_0 \in \{0, 1\}.$$

2. Let  $n = 2$ ,  $P = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ , and  $S = [S_0 \quad S_{X_1}]$ . The four possible values of  $A = [A_0 \quad A_1]$  are  $[0 \ 0]$ ,  $[0 \ 1]$ ,  $[1 \ 0]$ , and  $[1 \ 1]$ . The corresponding

values of  $S$  are  $[0 \ 0]$ ,  $[0 \ 1]$ ,  $[1 \ -1]$ , and  $[1 \ 0]$ . Hence

$$S_0 \in \{0, 1\}$$

and

$$S_{X_1} \in \{0, \pm 1\}.$$

3. Assume proposition is true for  $(n-1)$  variables and prove for  $n$  variables.

Case (i). Consider the component  $S_0 = (K; S^n)$ ,  $K=1$ . We know that  $p_{11} = 1$  and  $p_{i1} = 0$ ,  $i = 2, 3, \dots, 2^n$ . Since  $A_0 \in \{0, 1\}$  we have  $S_0 \in \{0, 1\}$ .

Case (ii). Consider the component  $(K; S^n)$ ,  $K = 2, 3, \dots, 2^{n-1}$ . Let  $(K; S^{n-1})$  have  $t_K$  subscripts. Then  $(K; S^n)$  also has  $t_K$  subscripts. By assumption  $(K; S^{n-1})$  takes values from  $\{0, \pm 1, \pm 2, \dots, \pm 2^{t_K-1}\}$ .

$$\text{Let } P_{2^n \times 2^n} = \left[ \begin{array}{c|c} D_1 & D_2 \\ \hline D_3 & D_4 \end{array} \right] \text{ and } A = [A' \ A''] \text{ where}$$

$$A' = [A_0 A_1 \dots A_{2^{n-1}-1}]$$

$$A'' = [A_{2^{n-1}} A_{2^{n-1}+1} \dots A_{2^n-1}]$$

$$D_1, D_4 = P_{2^{n-1} \times 2^{n-1}}$$

$$D_2 = -D_1$$

and

$$D_3 = 0.$$

$(K; S^n)$  is given by the sum of the  $k^{th}$  components of  $A'D_1$  and  $A''D_3$ . Since  $A''D_3 = 0$ ,  $(K; S^n)$  corresponds to some  $(K; S^{n-1})$  and hence takes values from  $\{0, \pm 1, \pm 2, \dots, \pm 2^{t_K-1}\}$ .

Case (iii). Consider the component  $(K; S^n)$ ,  $K = 2^{n-1}+1, 2^{n-1}+2, \dots, 2^n$ . Let  $(K-2^{n-1}; S^{n-1})$  have  $t'_K$  subscripts. Then  $(K; S^n)$  has  $(t'_K+1)$  subscripts.  $(K; S^n)$  is the sum of  $(K-2^{n-1})^{th}$  components of  $A'D_2$  and  $A''D_4$ . The  $(K-2^{n-1})^{th}$  component of  $A''(D_4)$  takes values from  $\{0, \pm 1, \pm 2, \dots, \pm 2^{t_K-1}\}$  and the  $(K-2^{n-1})^{th}$  component of  $A'D_2$  takes values from  $\{0, \bar{\pm} 1, \bar{\pm} 2, \dots, \bar{\pm} 2^{t'_K-1}\}$ . Hence  $(K; S^n)$  takes values from  $\{0, \pm 1, \pm 2, \dots, \pm 2^{t'_K}\}$ . ■ ■

Theorem 2.12: Let  $N = \{1, 2, \dots, n\}$ . Then

$$S_0 \in \{0, 1\}$$

$$S_0 + S_{X_i} \in \{0, 1\} \quad \forall i \in N$$

$$S_0 + S_{X_i} + S_{X_j} + S_{X_i X_j} \in \{0, 1\} \quad \forall i, j \in N \text{ and } i \neq j$$

$$S_0 + S_{X_i} + S_{X_j} + S_{X_K} + S_{X_i X_j} + S_{X_i X_K} + S_{X_j X_K} + S_{X_i X_j X_K} \in \{0, 1\}$$

$$\forall i, j, K \in N \text{ and } i \neq j \neq K$$

⋮

$$S_0 + S_{X_1} + S_{X_2} + \dots + S_{X_n} + S_{X_1 X_2} + S_{X_1 X_3} + \dots + S_{X_1 X_n}$$

$$+ S_{X_2 X_3} + S_{X_2 X_4} + \dots + S_{X_1 X_2 X_3} + \dots + S_{X_1 X_2 X_n} + \dots$$

$$+ S_{X_1 X_2 \dots X_n} \in \{0, 1\}.$$

Proof: 1. Consider  $n = 1$ ,  $S_0 \in \{0,1\}$ .

2. Consider  $n = 2$ . The possible values of  $S = [S_0 \ S_{X_1}]$  are  $[0 \ 0]$ ,  $[0 \ 1]$ ,  $[1 \ -1]$ , and  $[1 \ 0]$ . Hence  $S_0 + S_{X_1} \in \{0,1\}$ .

3. Assume true for  $(n-1)$  variables and prove for  $n$  variables. Hence we have

$$S_0 + S_{X_i} \in \{0,1\} \quad \forall i \in N - \{n\}$$

$$\begin{matrix} S_0 + S_{X_i} + S_{X_j} + S_{X_i X_j} \in \{0,1\} & \forall i,j \in N - \{n\} \text{ and } i \neq j \\ \vdots \end{matrix}$$

Case (i). Series with subscript  $X_1$  absent. We will consider the equation

$$S_0 + S_{X_i} + S_{X_j} + S_{X_i X_j}, \quad i,j \in N - \{n\} \quad \text{and} \quad i \neq j.$$

Let

$$S_0 = (a; S^n)$$

$$S_{X_i} = (b; S^n)$$

$$S_{X_j} = (c; S^n)$$

$$S_{X_i X_j} = (d; S^n).$$

Clearly

$$a, b, c, d \leq 2^{n-1}.$$

Let

$$A = [A' \ A''] \quad \text{and} \quad P = \left[ \begin{array}{c|c} D_1 & D_2 \\ \hline D_3 & D_4 \end{array} \right].$$



Since  $A''D_3 = 0$

$$S_0 + S_{X_i} + S_{X_j} + S_{X_i X_j} = \text{Sum of } a, b, c, \text{ and } d^{th} \text{ components of } A'D_1.$$

Since  $A'D_1$  is the spectrum of some Boolean function of  $(n-1)$  variables, the righthand side is  $S_0 + S_{X_{i-1}} + S_{X_{j-1}} + S_{X_{i-1} X_{j-1}}$  of  $(n-1)$  variables. Hence

$$S_0 + S_{X_i} + S_{X_j} + S_{X_i X_j} \in \{0, 1\}.$$

Similarly we can show that the series of the form

$$\begin{aligned} & S_0 + S_{X_i} + S_{X_j} + S_{X_K} + S_{X_i X_j} + S_{X_i X_K} + S_{X_j X_K} + S_{X_i X_j X_K}, \\ & \qquad \qquad \qquad i, j, K \in N - \{1\} \\ & S_0 + S_{X_i} + S_{X_j} + S_{X_K} + S_{X_\ell} + S_{X_i X_j} + S_{X_i X_K} + S_{X_i X_\ell} + S_{X_j X_K} + \dots \\ & \qquad \qquad \qquad + S_{X_i X_j X_K} + \dots + S_{X_i X_j X_K X_\ell} \qquad i, j, K, \ell \in N - \{1\} \\ & \qquad \qquad \qquad i \neq j \neq K \neq \ell \\ & \qquad \qquad \qquad \vdots \end{aligned}$$

take values from the set  $\{0, 1\}$ .

Case (ii). Series with subscript  $X_1$  present. We will consider the equation

$$S_0 + S_{X_1} + S_{X_j} + S_{X_1 X_j}, \quad j \in N \text{ and } j \neq 1.$$

Let

$$S_0 = (a; S^n)$$

$$S_{X_1} = (b; S^n)$$

$$S_{X_j} = (c; S^n)$$

$$S_{X_1 X_j} = (d; S^n).$$

We know that  $a, c \leq 2^{n-1}$ ,  $b = a + 2^{n+1}$ , and  $d = c + 2^{n-1}$ . Since  $A''D_3 = 0$

$$\begin{aligned} S_0 + S_{X_1} + S_{X_j} + S_{X_1 X_j} &= a^{th} \text{ component of } A'D_1 + c^{th} \\ &\text{component of } A'D_1 + (b-2^{n-1})^{th} \\ &\text{component of } A'D_2 + (b-2^{n-1})^{th} \\ &\text{component of } A''D_4 + (d-2^{n-1})^{th} \\ &\text{component of } A'D_2 + (d-2^{n-1})^{th} \\ &\text{component of } A''D_4. \end{aligned}$$

Since  $D_1 = -D_2$

$$(b-2^{n-1})^{th} \text{ component of } A'D_2 = -(a^{th} \text{ component of } A'D_1).$$

and

$$(d-2^{n-1})^{th} \text{ component of } A'D_2 = -(c^{th} \text{ component of } A'D_1).$$

$$\begin{aligned} S_0 + S_{X_1} + S_{X_j} + S_{X_1 X_j} &= (b-2^{n-1})^{th} \text{ component of} \\ &A''D_4 + (d-2^{n-1})^{th} \text{ component of} \\ &A''D_4. \end{aligned}$$

Hence

$$S_0 + S_{X_1} + S_{X_j} + S_{X_1 X_j} \in \{0, 1\}.$$

Similarly we can show that all series of the form

$$S_0 + S_{x_1} + S_{x_j} + S_{x_K} + S_{x_1 x_j} + S_{x_1 x_K} + S_{x_j x_K} + S_{x_1 x_j x_K},$$

$\vdots$

$$j, K \in N, \quad j \neq K$$

takes values from the set  $\{0,1\}$ .

## 2.4 RMC Expansion and Probability Transform

### 2.4.1 Introduction

In this section we study the relationship between the Ring sum (or Reed Muller canonic) expansion of a Boolean switching function and the corresponding probability expression.

The generalized Reed Muller canonic (RMC) expansion of a Boolean function of  $n$  variables is unique and is given by

$$\begin{aligned} f = & a_0 \oplus a_{x_1} \tilde{x}_1 \oplus a_{x_2} \tilde{x}_2 \oplus a_{x_n} \tilde{x}_n \oplus a_{x_1 x_2} \tilde{x}_1 \tilde{x}_2 \oplus \dots \\ & \oplus a_{x_1 x_2 \dots x_n} \tilde{x}_1 \tilde{x}_2 \dots \tilde{x}_n \end{aligned} \quad (2.8)$$

where  $\tilde{x}_i$  is either the complemented variable  $x_i$  or the complemented variable  $\bar{x}_i$ . Each variable appears in the expansion only in the complemented or the uncomplemented form but not in both. The RMC coefficient vector is defined by

$$\begin{aligned} a = & (a_0 a_{x_n} a_{x_{n-1}} a_{x_{n-1} x_n} a_{x_{n-2}} a_{x_{n-2} x_n} a_{x_{n-2} x_{n-1}} a_{x_{n-2} x_{n-1} x_n} \\ & \dots a_{x_1} a_{x_1 x_n} a_{x_1 x_{n-1}} \dots a_{x_1 x_2 \dots x_n}) \stackrel{\Delta}{=} (a_0 a_1 \dots a_{2^n-1}). \end{aligned}$$

Each  $a_j$  in expression (2.8) is a binary constant. The function  $f(x_1, x_2, \dots, x_n)$  can be realized by the circuit of Figure 2.3 where each AND gate forms a product term for a non-zero  $a_j$ .

#### 2.4.2 Relationship Between the Spectrum S and RMC Coefficients of a Boolean Function f

The set of elements  $\{0,1\}$  with the operations of Exclusive OR and AND forms a field. A vector space of dimension  $2^n$  can be defined over this field. Any switching function is a vector in this vector space and the terms in the RMC expansion form a basis for this space.

It has been shown in [Sw72] that for any arbitrary Boolean function

$$A^T = R_{2^n \times 2^n} \cdot a^T \quad (2.9)$$

where the basis matrix,  $R_{2^n \times 2^n}$ , is the matrix whose columns correspond to the  $2^n$  basis vectors. It has been shown in [Pr64] that  $R_{2^n \times 2^n}$  can be defined recursively as

$$R_{1 \times 1} = 1; R_{2^n \times 2^n} = \left[ \begin{array}{c|c} R_{2^{n-1} \times 2^{n-1}} & 0 \\ \hline R_{2^{n-1} \times 2^{n-1}} & R_{2^{n-1} \times 2^{n-1}} \end{array} \right].$$

In addition  $R_{2^n \times 2^n}$  is its own inverse. Hence we have

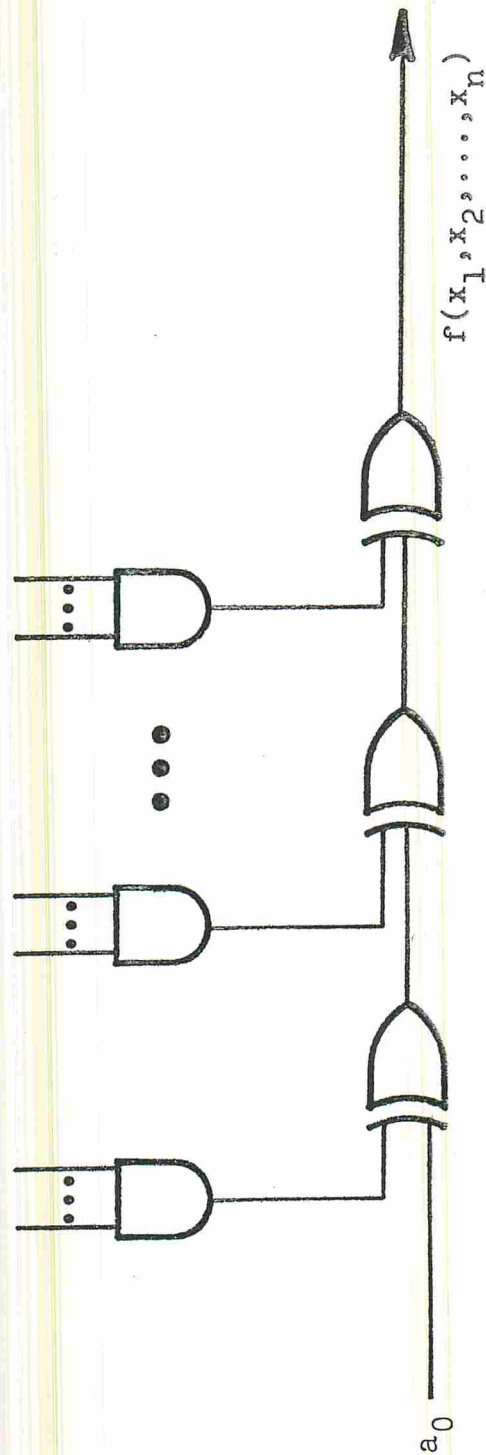


Figure 2.3. Reed Muller canonic realization of a Boolean function  $f$



$$a^T = R_{2^n \times 2^n} \cdot A^T. \quad (2.10)$$

Equivalently

$$a = A \cdot R_{2^n \times 2^n}^T \quad (2.11)$$

where

$$R_{2^n \times 2^n}^T = \left[ \begin{array}{c|c} R_{2^{n-1} \times 2^{n-1}}^T & R_{2^{n-1} \times 2^{n-1}}^T \\ \hline 0 & R_{2^{n-1} \times 2^{n-1}}^T \end{array} \right].$$

The next results relate our new spectrum vector  $S$  to the RMC coefficient vector  $a$ .

Theorem 2.13: Let  $S$  be the spectrum of a Boolean function  $f$  and  $a$  be the vector of coefficients of the RMC expansion. Then

$$|S|_{\text{mod } 2} = a.$$

Proof: Let  $r_{ij}$  and  $p_{ij}$  be the elements of  $R^T$  and  $P$  respectively. We will show that  $r_{ij} = |p_{ij}|$ . This is clearly true for  $n=1$  since  $R_{1 \times 1} = P_{1 \times 1} = 1$ , and for  $n=2$  since  $R_{2 \times 2}^T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  and  $P_{2 \times 2} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ .

Assume it is true for  $n$  and prove true for  $n+1$ .

$$R_{2^{n+1} \times 2^{n+1}}^T = \left[ \begin{array}{c|c} R_{2^n \times 2^n}^T & R_{2^n \times 2^n}^T \\ \hline 0 & R_{2^n \times 2^n}^T \end{array} \right]$$

$$P_{2^{n+1} \times 2^{n+1}} = \left[ \begin{array}{c|c} P_{2^n \times 2^n} & -P_{2^n \times 2^n} \\ \hline 0 & P_{2^n \times 2^n} \end{array} \right].$$

Since  $R_{2^n \times 2^n}^T = |P_{2^n \times 2^n}| = |-P_{2^n \times 2^n}|$ ,

$$R_{2^{n+1} \times 2^{n+1}}^T = |P_{2^{n+1} \times 2^{n+1}}|.$$

We know that

$$S = AP$$

and

$$a = AR^T.$$

Consider a component  $S_j$  of the spectrum  $S$ .

$$S_j = \sum A_i p_{ij}, \quad p_{ij} \in \{0, 1, -1\}$$

$$|S_j| = |\sum A_i p_{ij}|.$$

Let  $I$  be a set of integers  $i$  such that  $A_i = 1$ . Then

$$|S_j| = \left| \sum_{i \in I} p_{ij} \right|. \quad (2.12)$$

Let  $x$  be the number of  $p_{ij}$  such that

$$p_{ij} = 1 \quad \text{for } i \in I.$$

Let  $y$  be the number of  $p_{ij}$  such that

$$p_{ij} = -1 \quad \text{for } i \in I.$$

Let  $x = y + g$ . Then

$$|S_j| = |x - y| = |g|$$

and

$$|S_j|_{\text{mod } 2} = |g|_{\text{mod } 2}.$$

Consider the component  $a_j$  of the RMC expansion where  $a_j = \sum_i r_{ij}$  where  $r_{ij} = |p_{ij}|$ . Now  $a_j = \sum_{i \in I} r_{ij}$  where the summation is mod 2 and

$$a_j = (x + y) \text{ mod } 2. \quad (2.13)$$

Consider the following cases.

Case 1:  $x \geq y$  and  $x = y + g$  where  $g \geq 0$ . Then

$$\begin{aligned}
a_j &= (x+y) \bmod 2 \\
&= (2y+g) \bmod 2 \\
&= g \bmod 2 \\
&= |g|_{\bmod 2} .
\end{aligned}$$

Case 2:  $x \leq y$  and  $y = x+g$  where  $g \geq 0$

$$\begin{aligned}
a_j &= (x+y) \bmod 2 \\
&= (2x+g) \bmod 2 \\
&= g \bmod 2 \\
&= |g|_{\bmod 2} .
\end{aligned}$$

Hence  $|S_j|_{\bmod 2} = a_j$ . ■ ■

Theorem 2.13 indicates that the coefficients of the RMC expression can be derived easily from the spectrum  $S$  of a Boolean function  $f$ . A given coefficient in the RMC expression is 1 (0) if the corresponding coefficient in  $S$  is odd (even). The coefficients of  $S$  can be determined from the RMC expansion coefficients by using the equation

$$S = aR^TP$$

where  $aR^T$  is performed with mod 2 addition.

Given the spectrum  $S$ , the RMC coefficient vector  $a$  can be computed in  $2^n$  operations. However, obtaining  $S$  from the RMC coefficient vector requires a procedure of com-

plexity of  $O(n \cdot 2^n)$  operations.

Example 2.10: Consider the function  $f = \bar{x}_1 x_3 \vee x_2 x_3 \vee x_1 \bar{x}_2 \bar{x}_3$ .

The vector A is indicated in Figure 2.4.

The spectrum S of the function f is given by

$$S = [01011011] \begin{bmatrix} 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 0 & 1 & 0 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & -1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ & & & & & 1 & -1 & -1 & 1 \\ & & & & & 0 & 1 & 0 & -1 \\ & 0 & & & & 0 & 0 & 1 & -1 \\ & & & & & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= [01001-2-12]$$

and

$$F = X_1 - X_1 X_2 + X_3 - 2X_1 X_3 + 2X_1 X_2 X_3.$$

The RMC coefficients are given by

$$a = A \cdot R^T$$

where summation is mod 2.



$x_1$	$x_2$	$x_3$	A
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Figure 2.4. Vector A for  $f = \bar{x}_1 x_3 \vee x_2 x_3 \vee x_1 \bar{x}_2 \bar{x}_3$

$$a = [01011001] \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= [01001010].$$

Now  $S = [01001-2-12]$  and  $|S|_{\text{mod } 2} = [01001010] = a$ .  
Hence the RMC expression is given by

$$f = x_3 \oplus x_1 \oplus x_1 x_2.$$

### 2.4.3 Minimization of RMC Expansion

The generalized RMC expansion of a function  $f(x_1, x_2, \dots, x_n)$  is given by

$$f = a_0 \oplus a_{x_1} \tilde{x}_1 \oplus a_{x_2} \tilde{x}_2 \oplus \dots \oplus a_{x_n} \tilde{x}_n \oplus a_{x_1 x_2} \tilde{x}_1 \tilde{x}_2 \oplus \dots \\ \oplus a_{x_1 x_2 \dots x_n} \tilde{x}_1 \tilde{x}_2 \dots \tilde{x}_n.$$

It has been shown that there are  $2^n$  RMC forms of a function  $f(x_1, x_2, \dots, x_n)$ . In each form, each variable is uniformly complemented or uncomplemented.

Definition 2.9: The *polarity function*  $X$  of the RMC form of a function  $f$  is given by  $X = (\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_n)$ .

Minimizing the RMC expansion involves the selection of the polarity function that yields an RMC expansion for a function  $f$  with the least number of terms in it. Solutions for minimizing the RMC expansion have been presented in [MS70, SW72, SO78, DDT78].

We will now present a new method for minimizing the RMC expansion.

Theorem 2.14: Let  $F$  be a probability expression for the Boolean function  $f$  with polarity function  $X = (x_1, x_2, \dots, x_n)$  such that  $F = S_0 + S_{X_1} X_1 + S_{X_2} X_2 + \dots + S_{X_i} X_i + \dots + S_{X_1 X_i} X_1 X_i + \dots + S_{X_1 X_2 \dots X_n} X_1 X_2 \dots X_n$ . Then a probability expression for the function  $f$  with respect to the polarity function  $\tilde{X} = (x_1, x_2, \dots, \bar{x}_i, \dots, x_n)$  is given by

$$\begin{aligned} F = & (S_0 + S_{X_i}) + (S_{X_1} + S_{X_1 X_i}) X_1 + (S_{X_2} + S_{X_2 X_i}) X_2 + \dots - S_{X_i} \bar{X}_i \\ & + \dots + (S_{X_1 X_2} + S_{X_1 X_2 X_i}) X_1 X_2 + \dots - S_{X_1 X_2 X_i} X_1 X_2 \bar{X}_i \\ & + \dots + (S_{X_1 X_3} + S_{X_1 X_3 X_i}) X_1 X_3 + \dots - S_{X_1 X_3 X_i} X_1 X_3 \bar{X}_i \dots \end{aligned}$$

$$\text{where } \bar{X}_i = \Pr(\bar{x}_i = 1). \quad (2.15)$$

Proof: Consider all terms containing the variable  $X_i$  in the probability expression  $F$ . A typical term is

$$S_{X_1 X_2 \dots X_i X_1 X_2 \dots X_i}.$$

$$\begin{aligned} S_{X_1 X_2 \dots X_i X_1 X_2 \dots X_i} &= S_{X_1 X_2 \dots X_i X_1 X_2 \dots X_{i-1} (1-1+X_i)} \\ &= S_{X_1 X_2 \dots X_i X_1 X_2 \dots X_{i-1} [1-(1-X_i)]} \\ &= S_{X_1 X_2 \dots X_i X_1 X_2 \dots X_{i-1} [1-\bar{X}_i]} \\ &= (S_{X_1 X_2 \dots X_i X_1 X_2 \dots X_{i-1}}) \\ &\quad - (S_{X_1 X_2 \dots X_i X_1 X_2 \dots \bar{X}_i}). \end{aligned} \quad (2.16)$$

Thus every term containing the variable  $X_i$  is split into two components of Equation (2.16). Hence the coefficient of the term  $X_1 X_2 \dots X_{i-1}$  in a probability expression  $F$  with the new polarity function  $\tilde{X} = (x_1, x_2, \dots, \bar{x}_i, \dots, x_n)$  is given by

$$(S_{X_1 X_2 \dots X_{i-1}} + S_{X_1 X_2 \dots X_i})$$

and the coefficient of the term  $X_1 X_2 \dots \bar{X}_i$  is given by  $-S_{X_1 X_2 \dots X_i}$  and Equation (2.15) follows immediately. ■■

Definition 2.10: The spectrum of a Boolean function  $f$  with respect to the polarity function  $X$  is denoted by  $S_X$ .

It follows from Definition 2.10 that  $\left| S_{\tilde{X}} \right|_{\text{mod } 2}$  is the set of coefficients of the RMC expansion of the function  $f$  with respect to the polarity function  $\tilde{X}$ .

Example 2.11: Consider the function  $f = x_1 x_2$

$$F = X_1 X_2$$

ans  $S_X = [0 \ 0 \ 0 \ 1]$  where  $X = (x_1, x_2)$ . If we change the polarity function to  $\tilde{X} = (\bar{x}_1, x_2)$  then  $F = [1 - \bar{x}_1]X_2 = X_2 - \bar{x}_1 X_2$  where  $\bar{x}_1 = \Pr(\bar{x}_1=1)$  and  $S_{\tilde{X}} = [0 \ 1 \ 0 \ -1]$  and  $a_{\tilde{X}} = \left| S_{\tilde{X}} \right|_{\text{mod } 2} = [0 \ 1 \ 0 \ 1]$ . The RMC expansion is  $x_2 \oplus \bar{x}_1 x_2$ .

#### 2.4.3.1 Procedure to Generate the Minimal RMC Form

We will now present a procedure to determine the minimal RMC form of a Boolean function. The  $2^n$  polarity functions will be generated in a gray code sequence. Table 2.2 shows the 3-bit gray code and the corresponding polarity functions. This can be generalized to the n-bit gray code and its associated polarity functions.

Table 2.2. Gray Codewords and Corresponding Polarity Function of 3 Variables

GRAY CODE	POLARITY FUNCTION
111	$\tilde{X}_1 = (x_1, x_2, x_3)$
101	$\tilde{X}_2 = (x_1, \bar{x}_2, x_3)$
100	$\tilde{X}_3 = (x_1, \bar{x}_2, \bar{x}_3)$
000	$\tilde{X}_4 = (\bar{x}_1, \bar{x}_2, \bar{x}_3)$
001	$\tilde{X}_5 = (\bar{x}_1, \bar{x}_2, x_3)$
011	$\tilde{X}_6 = (\bar{x}_1, x_2, x_3)$
010	$\tilde{X}_7 = (\bar{x}_1, x_2, \bar{x}_3)$
110	$\tilde{X}_8 = (x_1, x_2, \bar{x}_3)$



Procedure 2.2:

1. Obtain  $A = [A_0 \ A_1 \ \dots \ A_{2^n-1}]$ .
2. Generate  $S_{\tilde{X}_1} = AP$ . Let  $T_1$  be the number of entries in  $S_{\tilde{X}_1}$  that are odd.
3. Compute  $S_{\tilde{X}_i}$ ,  $i = 2, 3, \dots, 2^n$  for the remaining  $2^n - 1$  polarity functions in the gray code sequence using Theorem 2.14. Calculate the number of entries  $T_i$  in  $S_{\tilde{X}_i}$ .
4. The minimal form of the RMC expansion corresponds to the polarity function  $\tilde{X}_j$  such that  $T_j = \min_i T_i$ ,  $i = 1, 2, \dots, 2^n$ .

Example 2.12: Consider the function  $f = x_1 \bar{x}_3 \vee x_1 x_2 \vee \bar{x}_1 \bar{x}_2 x_3$ .

The A vector =  $[0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1]$ .

$$\begin{aligned} 1. \quad S_{\tilde{X}_1} = AP &= [S_0 S_{x_3} S_{x_2} S_{x_2 x_3} S_{x_1} S_{x_1 x_3} S_{x_1 x_2} S_{x_1 x_2 x_3}] \\ &= [0 \ 1 \ 0 \ -1 \ 1 \ -2 \ 0 \ 2] \end{aligned}$$

and  $T_1 = 3$ .

$$\begin{aligned} 2. \quad \text{Compute } S_{\tilde{X}_2} &= [\tilde{S}_0 \tilde{S}_{x_3} \tilde{S}_{\bar{x}_2} \tilde{S}_{\bar{x}_2 x_3} \tilde{S}_{x_1} \tilde{S}_{x_1 x_3} \tilde{S}_{x_1 \bar{x}_2} \tilde{S}_{x_1 \bar{x}_2 x_3}] \\ \text{where } \tilde{X}_2 &= (x_1, \bar{x}_2, x_3) \end{aligned}$$

$$\tilde{s}_0 = s_0 + s_{x_2} = 0$$

$$\tilde{s}_{x_3} = s_{x_2 x_3} + s_{x_3} = 0$$

$$\tilde{s}_{\bar{x}_2} = -s_{x_2} = 0$$

$$\tilde{s}_{\bar{x}_2 x_3} = -s_{x_2 x_3} = 1$$

$$\tilde{s}_{x_1} = s_{x_1} + s_{x_1 x_2} = 1$$

$$\tilde{s}_{x_1 x_3} = s_{x_1 x_3} + s_{x_1 x_2 x_3} = 0$$

$$\tilde{s}_{x_1 \bar{x}_2} = -s_{x_1 x_2 x_3} = -2$$

and

$$T_2 = 2.$$

Similarly we have

$$s_{\tilde{x}_3} = [0 \quad 0 \quad 1 \quad -1 \quad 1 \quad 0 \quad -2 \quad 2]; T_3 = 3$$

$$s_{\tilde{x}_4} = [1 \quad 0 \quad -1 \quad 1 \quad -1 \quad 0 \quad 2 \quad -2]; T_4 = 4$$

$$s_{\tilde{x}_5} = [1 \quad 0 \quad 0 \quad -1 \quad -1 \quad 0 \quad 0 \quad 2]; T_5 = 3$$

$$s_{\tilde{x}_6} = [1 \quad -1 \quad 0 \quad 1 \quad -1 \quad 2 \quad 0 \quad -2]; T_6 = 4$$

$$s_{\tilde{x}_7} = [0 \quad 1 \quad 1 \quad -1 \quad 1 \quad -2 \quad -2 \quad 2]; T_7 = 4$$

$$s_{\tilde{x}_8} = [1 \quad -1 \quad -1 \quad 1 \quad -1 \quad 2 \quad 2 \quad -2]; T_8 = 5.$$

The minimal RMC form corresponds to the polarity function  $\tilde{X}_2$  expression is  $x_1 \oplus \bar{x}_2 x_3$ .

#### 2.4.3.2 Complexity Analysis

The procedures presented in [MS70, Sw72, and S078] perform computations of the form  $a = A \cdot R^T$  for a given polarity function. To determine all the canonic forms it is necessary to consider the appropriate basis matrices or rearranged  $f$  vectors before carrying out the computations.

Theorem 2.15: The computational complexity of determining the minimal RMC forms by the procedures described in [MS70, Sw72, S078] is  $O(n2^{2n})$ .

Proof: There are  $2^n$  polarity functions for any function of  $n$  variables. For each polarity function a computation of the form  $a = AR^T$  is needed. From the structure of  $R^T$  and by using Theorem 2.8 we can show that each computation of the form  $a = AR^T$  is  $O(n \cdot 2^n)$  additions and hence the total complexity is  $O(n \cdot 2^{2n})$  additions. ■ ■

The computational complexity of the algorithms for determining the minimal RMC form of a Boolean function presented in [DDT78] is  $O(2^{2n})$ .

Theorem 2.16: The computational complexity of Procedure 2.2 is  $O(2^{2n})$ .

Proof: The change of any one variable in the polarity function results in at most  $2^{n-1}$  additions and  $2^{n-1}$  changes of sign in computing the new spectrum. Since there are  $2^n$  polarity functions, the complexity of the procedure is  $O(2^{2n})$ . ■ ■

In this section we have established the relationship between the spectrum  $S$  and coefficients of the RMC expression for a given function  $f$ .

## 2.5 Walsh Transform and Probability Transform

The Walsh transform is a method of describing a Boolean function by a set of  $2^n$  integers where  $n$  is the number of variables in the function.

The transform description of a Boolean function  $f$  is a unique vector  $C$  of  $2^n$  integers.  $C$  is defined by the matrix multiplication  $C = W \cdot G^T$  where  $W$  is the Walsh matrix of order  $2^n \times 2^n$  and  $G$  is a vector of  $2^n$  integers representing  $f$ .

A formal mathematical description of the Walsh transform is presented by Walsh [Wa23].

Definition 2.11: The vector  $G$  is defined by  $G = [g_0, g_1, \dots, g_{2^n-1}]$  where

$$g_i = 1 \text{ if and only if the } i^{th} \text{ minterm } A_i = 0$$

$$g_i = -1 \text{ if and only if the } i^{th} \text{ minterm } A_i = 1.$$

For a function  $f(x_1, x_2, x_3)$  the Walsh coefficients  $C = [C(0), C(x_1), \dots, C(x_1 x_2 x_3)]^T$  are defined by

$$C = W_{8 \times 8} \cdot G^T$$

and the value of  $C(\cdot)$ , a term in  $C$ , is given by

$$C(\cdot) = \sum_{j=0}^7 w(\cdot, j) \cdot g_j.$$

Example 2.13: Computation of  $C$  vector.

Consider the function  $f(x_1, x_2, x_3) = x_1 x_2 \vee \bar{x}_1 x_3 \vee x_1 \bar{x}_3$ .

The vector  $A = (0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1)$  and  $G = (1 \ -1 \ 1 \ -1 \ -1 \ 1 \ -1 \ -1)$ .

The Walsh matrix of order 8 is shown in Figure 2.5.

Row								
0	1	1	1	1	1	1	1	$w(0)$
1	1	1	1	1	-1	-1	-1	$w(x_1)$
2	1	1	-1	-1	1	1	-1	$w(x_2)$
3	1	-1	1	-1	1	-1	1	$w(x_3)$
4	1	1	-1	-1	-1	-1	1	$w(x_1 x_2)$
5	1	-1	1	-1	-1	1	1	$w(x_1 x_3)$
6	1	-1	-1	1	1	-1	1	$w(x_2 x_3)$
7	1	-1	-1	1	-1	1	-1	$w(x_1 x_2 x_3)$

Figure 2.5. Walsh matrix of order 8



$$C(0) = \sum_{j=0}^7 w(0,j) \cdot g_j = -2$$

$$C(x_1) = \sum_j w(x_1,j) \cdot g_j = 2$$

$$C(x_2) = \sum_j w(x_2,j) \cdot g_j = 2$$

$$C(x_3) = \sum_j w(x_3,j) \cdot g_j = 2$$

$$C(x_1 x_2) = \sum_j w(x_1 x_2, j) \cdot g_j = -2$$

$$C(x_1 x_3) = \sum_j w(x_1 x_3, j) \cdot g_j = 6$$

$$C(x_2 x_3) = \sum_j w(x_2 x_3, j) \cdot g_j = -2$$

$$C(x_1 x_2 x_3) = \sum_j w(x_1 x_2 x_3, j) = 2$$

$$C = [-2 \quad 2 \quad 2 \quad 2 \quad -2 \quad 6 \quad -2 \quad 2]^T.$$

The vector  $G$  can be computed from the equation

$$G^T = \frac{1}{2^n} [W_{2^n \times 2^n}]^T \cdot C.$$

The Walsh transform can be computed rapidly on digital computers. A fast Walsh transform algorithm, described in [Sh69] requires  $n \cdot 2^n$  arithmetic operations. The Walsh

transform coefficients have been used in the classification of Boolean functions [De65,Ed75,Le71], in logic network design [Ed75,Hu73,Hu77,EH78,Le71,MH78] and in fault diagnosis [BH78,Ma77].

### 2.5.1 Relation Between the Spectrum S and the Walsh Coefficients of a Boolean Function f

We shall now establish the relationship between the spectrum S and the Walsh coefficients of a Boolean function f, thereby enabling any analysis to be carried out in either domain.

Theorem 2.17: Let S and C be the spectrum and Walsh coefficients of a Boolean function f of n variables. Then  $C = D_1 - D_2 S^T$  where  $D_1 = [2^n \ 0 \ 0 \ \dots \ 0]^T$  and  $D_2 = 2W \cdot (P^{-1})^T$ .

Proof: We know that

$$C = W \cdot G^T$$

$$G = \vec{1} - 2A$$

and

$$A = SP^{-1}$$

where  $\vec{1}$  is a vector of ones of dimension  $2^n$ .

$$\begin{aligned}
C &= W \cdot G^T \\
&= W[\vec{1} - 2A]^T \\
&= W \cdot \vec{1}^T - W \cdot 2A^T \\
&= W \cdot \vec{1}^T - 2W \cdot (S \cdot P^{-1})^T \\
&= W \cdot \vec{1}^T - 2W \cdot (P^{-1})^T \cdot S^T.
\end{aligned}$$

There are  $2^n$  ones in row zero of a Walsh matrix of order  $2^n$ . All other rows have  $2^{n-1}$  entries = 1 and  $2^{n-1}$  entries = -1. Hence  $W \cdot \vec{1}^T = [2^n \ 0 \ 0 \ \dots \ 0]^T$  and the result follows. ■■

Example 2.14: Consider the function

$$f = x_1 x_2 \vee \bar{x}_1 x_3 \vee x_1 \bar{x}_3$$

$$S = A \cdot P = [0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1]$$

$$\begin{bmatrix}
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\
0 & 1 & 0 & -1 & 0 & -1 & 0 & 1 \\
0 & 0 & 1 & -1 & 0 & 0 & -1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\
& & & & 1 & -1 & -1 & 1 \\
& & 0 & & 0 & 1 & 0 & -1 \\
& & & & 0 & 0 & 1 & -1 \\
& & & & 0 & 0 & 0 & 1
\end{bmatrix}$$

$$S = [0 \ 1 \ 0 \ 0 \ 1 \ -2 \ 0 \ 1]$$

$$W_{8 \times 8} \cdot (P_{8 \times 8}^{-1})^T = \begin{bmatrix} 8 & 4 & 4 & 2 & 4 & 2 & 2 & 1 \\ 0 & 0 & 0 & 0 & -4 & -2 & -2 & -1 \\ 0 & 0 & -4 & -2 & 0 & 0 & -2 & -1 \\ 0 & -4 & 0 & -2 & 0 & -2 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

and

$$2 \cdot W_{8 \times 8} \cdot (P_{8 \times 8}^{-1})^T \cdot S^T = 2 \begin{bmatrix} 5 \\ -1 \\ -1 \\ -1 \\ 1 \\ -3 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 10 \\ -2 \\ -2 \\ -2 \\ 2 \\ -6 \\ 2 \\ -2 \end{bmatrix}.$$

$$\begin{aligned} \text{Hence } D &= [80000000]^T - [10 \ -2 \ -2 \ -2 \ 2 \ -6 \ 2 \ -2]^T \\ &= [-2 \ 2 \ 2 \ 2 \ -2 \ 6 \ -2 \ 2]^T \end{aligned}$$

which is the same as derived in Example 2.13.

Theorem 2.18: Let  $S$  and  $C$  be the spectrum and Walsh coefficients of the Boolean function  $f$ . Then  $S = E_1 - \frac{1}{2^{n+1}} C^T E_2$  where  $E_1 = [\frac{1}{2} \ 0 \ 0 \ \dots \ 0]$  and  $E_2 = WP$ .

Proof: We know that

$$G^T = \frac{1}{2^n} W^T \cdot C$$

$$A = \frac{1}{2} [\vec{1} - G]$$

and

$$S = AP.$$

It can be seen that

$$G = \frac{1}{2^n} C^T W$$

and

$$\begin{aligned}
S &= \frac{1}{2} [\vec{1}-G]P \\
&= \frac{1}{2} [\vec{1}P] - \frac{1}{2} GP \\
&= \frac{1}{2} [\vec{1}P] - \frac{1}{2} \cdot \frac{1}{2^n} C^T_{WP}.
\end{aligned}$$

Since  $\frac{1}{2} [\vec{1}P] = [\frac{1}{2} 0 0 \dots 0]$

$$S = E_1 - \frac{1}{2^{n+1}} C^T E_2.$$

Example 2.15: Consider the previous example. Let  $C^T =$

$$[-2 \ 2 \ 2 \ 2 \ -2 \ 6 \ -2 \ 2],$$

$$WP = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \end{bmatrix} \begin{bmatrix} 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & -1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & -1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & -1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & -1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -2 & 0 & 0 & 0 \\ 1 & 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & -2 & 0 & -2 & 0 & 4 & 0 \\ 1 & -2 & 0 & 0 & -2 & 4 & 0 & 0 \\ 1 & -2 & -2 & 4 & 0 & 0 & 0 & 0 \\ 1 & -2 & -2 & 4 & -2 & 4 & 4 & -8 \end{bmatrix}$$

$$C^T_{WP} = [8 \ -16 \ 0 \ 0 \ -16 \ 32 \ 0 \ -16]$$



$$S = \begin{bmatrix} \frac{1}{2} & 0 & 0 & \cdots & 0 \end{bmatrix} - \frac{1}{16} \begin{bmatrix} 8 & -16 & 0 & 0 & -16 & 32 & 0 & -16 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & -2 & 0 & 1 \end{bmatrix}.$$

### 2.5.2 Computational Complexity

Theorem 2.19: The computation of  $C$  by  $C = D_1 - D_2 \cdot S^T$  is  $O(n \cdot 2^n)$  operations.

Proof:  $D_1$  and  $D_2$  can be precomputed for any  $n$ , and hence do not contribute to the computation time. The computation of  $D_2 S^T$  requires  $O(n \cdot 2^n)$  additions and hence  $C = D_1 - D_2 S^T$  is computed in  $O(n \cdot 2^n)$  operations. ■ ■

## 2.6 Probability Transform Domain Analysis of Boolean Functions

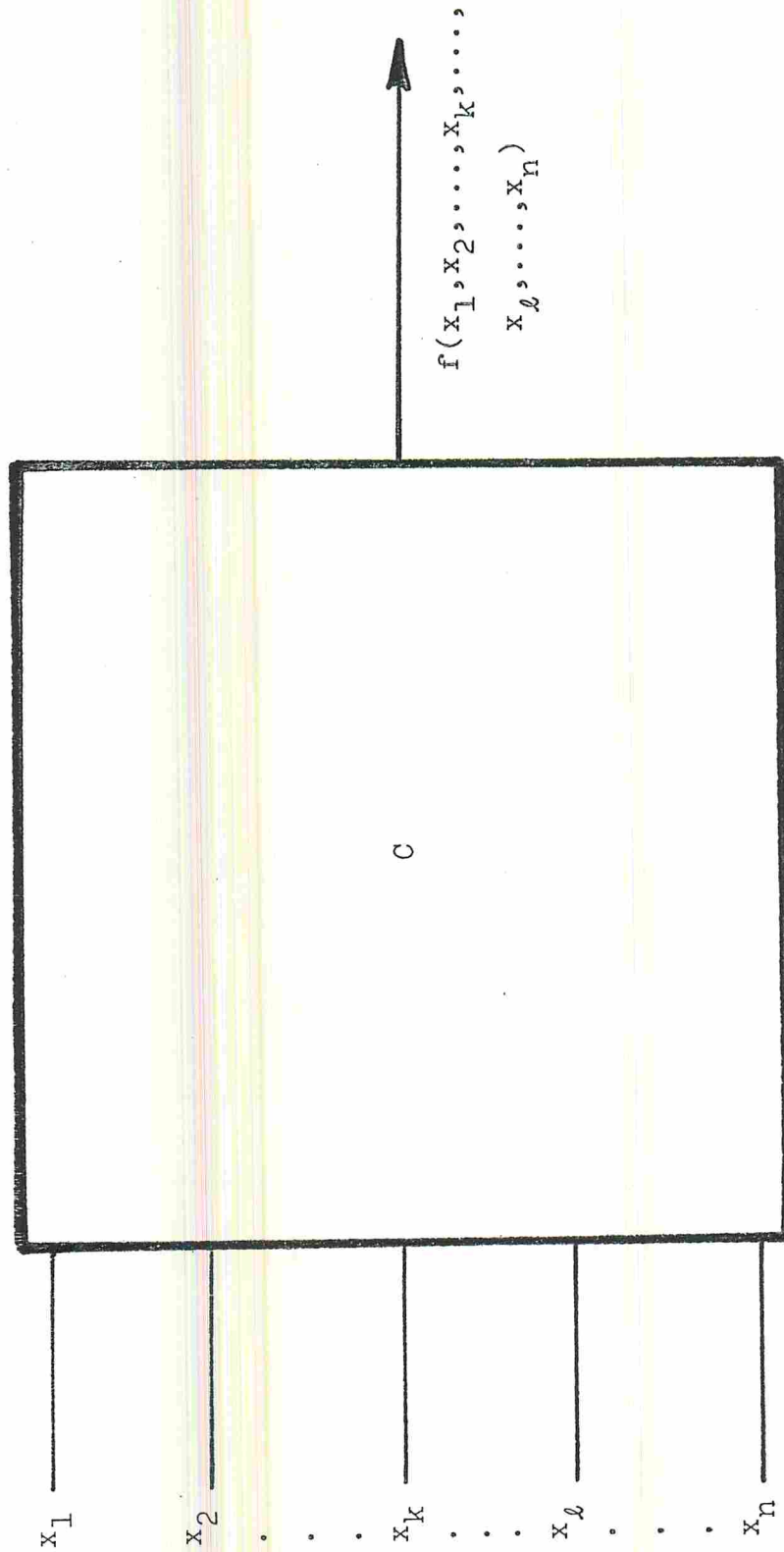
In this section we shall establish the relationship between operations in the probability transform domain which correspond to mappings between two Boolean functions.

Dertouzos [De75] and Edwards [Ed75] have derived certain operations in the Walsh transform domain which correspond to mappings between two Boolean functions. These operations have been applied to Boolean function classification and logic synthesis procedures.

We shall also study other properties of Boolean functions by examining the probability transform spectrum  $S$ .

### 2.6.1 Mapping Between Boolean Functions

Figure 2.6 represents the original function



$$S = [S_{b_0} S_{b_1} \dots S_{b_{2^n-1}}]$$

Figure 2.6. Function  $f$  and its spectrum  $S$

$f(x_1, x_2, \dots, x_k, \dots, x_\ell, \dots, x_n)$  and its spectrum  $S$ .

Mapping 1: Interchange of  $x_k$  and  $x_\ell$ ,  $k \neq \ell$  (Figure 2.7).

The new spectrum  $S'$  for  $f$  can be generated as follows

$$S' = [S_{b'_0}, S_{b'_1}, \dots, S_{b'_{2^n-1}}]$$

where  $b'_i$  is obtained by replacing the subscript  $k$  with subscript  $\ell$  (and vice versa) in  $b_i$  for all  $i$ .

Example 2.16: Consider the Boolean function  $f = x_1 x_2 \vee x_1 \bar{x}_3$

$$B = [1 \quad x_3 \quad x_2 \quad x_2 x_3 \quad x_1 \quad x_1 x_3 \quad x_2 x_3 \quad x_1 x_2 x_3]$$

$$\begin{aligned} S &= [S_1 \quad S_{x_3} \quad S_{x_2} \quad S_{x_2 x_3} \quad S_{x_1} \quad S_{x_1 x_3} \quad S_{x_1 x_2} \quad S_{x_1 x_2 x_3}] \\ &= [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad -1 \quad 0 \quad 1]. \end{aligned}$$

Interchange variables  $x_1, x_2$ .

The  $S'$  for the function  $f' = x_1 x_2 \vee x_2 \bar{x}_3$  is given by

$$\begin{aligned} S' &= [S_1 \quad S_{x_3} \quad S_{x_1} \quad S_{x_1 x_3} \quad S_{x_2} \quad S_{x_2 x_3} \quad S_{x_1 x_2} \quad S_{x_1 x_2 x_3}] \\ &= [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad -1 \quad 0 \quad 1]. \end{aligned}$$

Mapping 2: Complementation of the function  $f$ .

The operation is shown in Figure 2.8. The new spectrum  $S'$  can be generated by reversing the signs of all coefficients except  $S_0$ .  $S'_0 = 1 - S_0$ .

Example 2.17: Consider  $f = x_1 x_2 \vee x_1 \bar{x}_3$  of the previous example

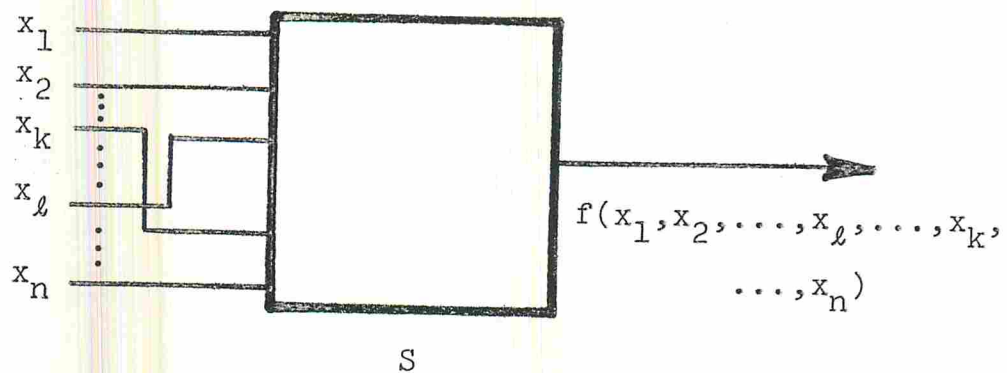


Figure 2.7. Interchange of variables  $x_k$  and  $x_l$

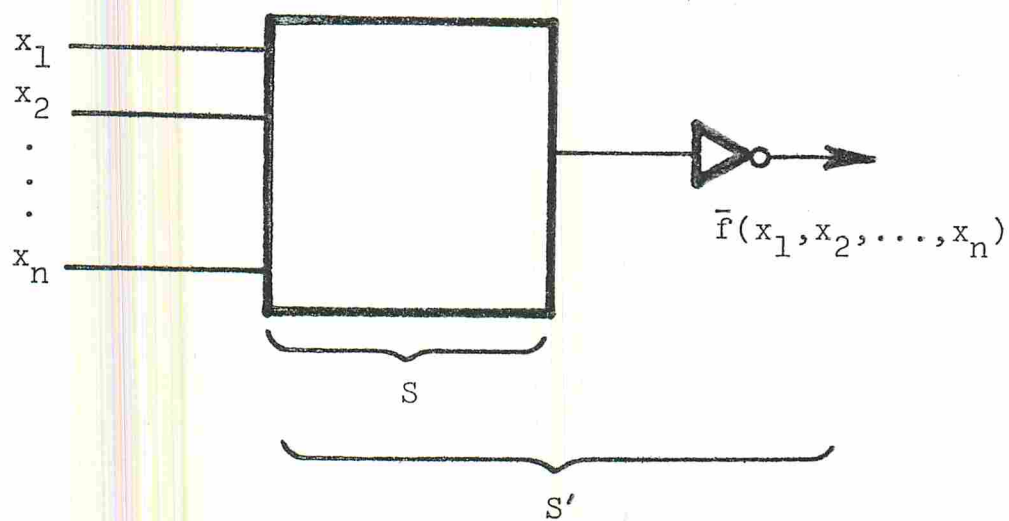


Figure 2.8. Spectrums  $S, S'$  for the functions  $f$  and  $\bar{f}$

$$S = [0 \ 0 \ 0 \ 0 \ 1 \ -1 \ 0 \ 1].$$

The spectrum  $S'$  for the function  $\bar{f}$  is given by

$$S' = [1 \ 0 \ 0 \ 0 \ -1 \ 1 \ 0 \ -1].$$

Mapping 3: Complementation of the variable  $x_k$ .

The operation is shown in Figure 2.9. The new spectrum  $S' = [S'_{b_0} \ S'_{b_1} \ \dots \ S'_{b_{2^n-1}}]$  is generated as follows.

Define a set  $I$  such that  $b_i \in I$  if and only if  $b_i$  contains the variable  $x_k$ . Then

$$S'_{b_i} = -S_{b_i} \quad \text{if } b_i \in I$$

$$S'_{b_i} = S_{b_i} + S_{b_i x_k} \quad \text{if } b_i \notin I.$$

Example 2.18: Consider  $f = x_1 x_2 \vee x_1 \bar{x}_3$ .

$$\begin{aligned} S &= [S_1 \ S_{x_3} \ S_{x_2} \ S_{x_2 x_3} \ S_{x_1} \ S_{x_1 x_3} \ S_{x_1 x_2} \ S_{x_1 x_2 x_3}] \\ &= [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ -1 \ 0 \ 1]. \end{aligned}$$

Change the variable  $x_1$  to  $\bar{x}_1$ .

$$I = \{x_1, x_1 x_3, x_1 x_2, x_1 x_2 x_3\}.$$

Hence

$$S'_{x_1} = -S_{x_1} = -1$$



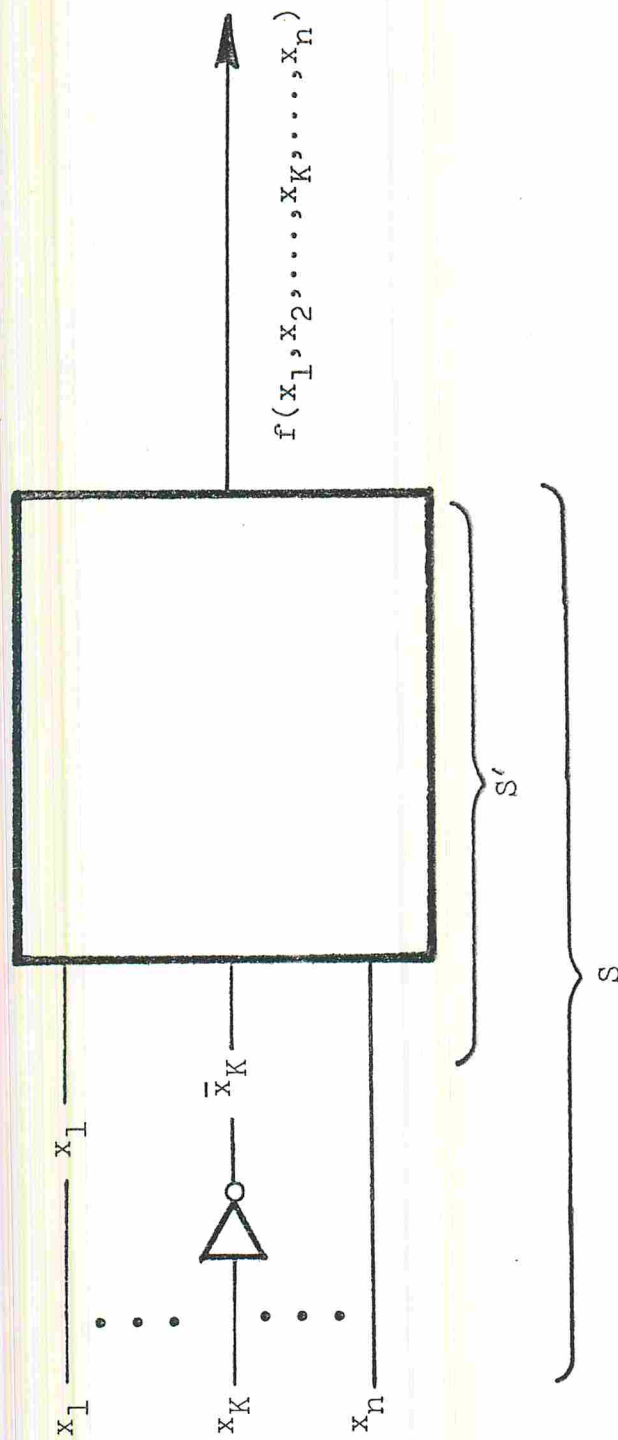


Figure 2.9. Complementation of variable  $x_K$

$$S'_{x_1 x_3} = -S_{x_1 x_3} = 1$$

$$S'_{x_1 x_2} = -S_{x_1 x_2} = 0$$

$$S'_{x_1 x_2 x_3} = -S_{x_1 x_2 x_3} = -1$$

$$S'_1 = S_1 + S_{x_1} = 1$$

$$S'_{x_3} = S_{x_3} + S_{x_1 x_3} = -1$$

$$S'_{x_2} = S_{x_2} + S_{x_1 x_2} = 0$$

$$S'_{x_2 x_3} = S_{x_2 x_3} + S_{x_1 x_2 x_3} = 1$$

Hence,  $S' = [1 \ -1 \ 0 \ 1 \ -1 \ 1 \ 0 \ -1]$

which is the spectrum of  $f' = \bar{x}_1 x_2 \vee \bar{x}_1 x_3$ .

## 2.6.2 Analysis of Properties of Boolean Functions

In this section we will study the properties of Boolean functions by examining the probability transform spectrum  $S$ . The main motivation is to identify classes of Boolean functions in the probability transform domain, enabling design engineers to use such analysis while designing circuits. We will mainly consider linear and unate functions as these functions have nice properties from the viewpoint of digital testing.

Definition 2.12: A function  $f(x_1, x_2, \dots, x_n)$  is said to be linear if it can be expressed as

$$f(x_1, x_2, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n$$

where  $a_i = 0$  or  $1$  for  $i = 0, 1, \dots, n$ .

A realization of a linear function is a linear circuit.

Definition 2.13: A function  $f(x_1, x_2, \dots, x_i, \dots, x_n)$  is said to be positive in the variable  $x_i$ , if for all  $2^{n-1}$  possible combinations of the values of the remaining  $(n-1)$  variables  $f(x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) \geq f(x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)$ . Similarly,  $f$  is negative in the variable  $x_i$ , if  $f(x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n) \geq f(x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n)$ .

Definition 2.14: A function  $f(x_1, x_2, \dots, x_n)$  is unate if for every variable  $x_i$ ,  $f$  is either positive or negative in the variable  $x_i$ .

All single faults in a linear function realized as a multilevel tree of two input exclusive OR elements can be detected by 4 tests. Betancourt [Be71] has shown that for any realization of a unate function containing only AND and OR gates all stuck faults can be detected by a universal test set  $T = \{S_0, S_1\}$  where  $S_0$  and  $S_1$  are the maximal 0 points and the minimal 1 points of the function.

Theorem 2.20: Let  $S = [S_{b_0}, S_{b_1}, \dots, S_{b_{2^n-1}}]$  be the spectrum of a Boolean function  $f(x_1, x_2, \dots, x_n)$ . Define a set  $I = \{b_0, b_i\}$  such that  $b_i \in I$  if and only if  $b_i$  contains only

one variable  $x_K$  (clearly, the cardinality of set  $I = n+1$ , where  $n$  = number of variables). Then the function  $f$  is linear if and only if

$$\left| S_{b_i} \right|_{\text{mod } 2} = 0, \quad b_i \notin I.$$

Proof: From Theorem 2.13 we know that

$$|S|_{\text{mod } 2} = a.$$

(1) Assume  $f$  linear. Then  $f = a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n \oplus$  with  $a_j = 0$  for terms of the form  $x_1 x_2, x_1 x_3, \dots, x_1 x_2 \dots x_n$ . The corresponding terms in  $S$  are of the form  $S_{b_i}$ ,  $b_i \notin I$  such that  $\left| S_{b_i} \right|_{\text{mod } 2} = 0$ .

(2)  $\left| S_{b_i} \right|_{\text{mod } 2} = 0$ ,  $b_i \notin I$  implies that the corresponding terms are absent in the RMC expansion and hence  $f$  is linear. ■ ■

The complexity of identifying a linear function by a procedure based on Theorem 2.20 is comparable to the complexity of deriving the RMC expression to determine if a function is linear or not.

Example 2.19: Consider the function  $f = x_1 x_2 \vee \bar{x}_1 \bar{x}_2$

$$S = [S_1 \ S_{x_2} \ S_{x_1} \ S_{x_1 x_2}] = [1 \ -1 \ -1 \ 2]$$

$$I = [1, X_2, X_1].$$

Since  $\left| S_{X_1 X_2} \right|_{\text{mod } 2} = 0$ ,  $f$  can be realized as a linear function. Since  $|S|_{\text{mod } 2} = [1 \ 1 \ 1 \ 0]$

$$f = 1 \oplus x_2 \oplus x_1.$$

Let us denote  $F(X_1, X_2, \dots, X_{i-1}, X_i = 1(0), X_{i+1}, \dots, X_n)$  by  $F|_{X_i=1(0)}$  for subsequent discussion.  $X_i$  and  $x_i$  both take value  $a_i \in \{0, 1\}$ .

Theorem 2.21:  $\left( F|_{X_i=1(0)} - F|_{X_i=0(1)} \right) \geq 0$  if and only if  $f$  is positive (or negative) in variable  $x_i$ .

1. Assume  $F|_{X_i=1} - F|_{X_i=0} \geq 0$ .

It follows that  $F|_{X_i=1} \geq F|_{X_i=0}$ . From Theorem 2.3

$$F|_{X_i=1} = f(x_1, x_2, \dots, x_i=1, \dots, x_n)$$

when  $X_j = x_j$  for  $j = 1, 2, \dots, i-1, i+1, \dots, n$ . Both  $X_j$  and  $x_j$  take values from the set  $\{0, 1\}$ . Therefore

$$f(x_1, x_2, \dots, x_i=1, \dots, x_n) \geq f(x_1, x_2, \dots, x_i=0, \dots, x_n)$$

and  $f$  is positive unate in  $x_i$ .

2. Assume  $f$  is positive unate in  $x_i$  then  $f(x_1, x_2, \dots, x_i=1, \dots, x_n) \geq f(x_1, x_2, \dots, x_i=0, \dots, x_n)$ . From the



assumption we can write

$$f = x_i f_1 \vee f_2$$

where  $f_1, f_2$  are functions independent of the variable  $x_i$ .

Hence

$$f(x_1, x_2, \dots, x_i=1, \dots, x_n) = f_1 + f_2$$

and

$$f(x_1, x_2, \dots, x_i=0, \dots, x_n) = f_2$$

$$\Pr(f_1 + f_2 = 1) \geq \Pr(f_2 = 1)$$

and hence

$$F|_{X_i=1} \geq F|_{X_i=0}$$

and

$$\left( F|_{X_i=1} - F|_{X_i=0} \right) \geq 0.$$

We can similarly show that  $\left( F|_{X_i=0} - F|_{X_i=1} \right) \geq 0$  if and only if  $f$  is negative in the variable  $x_i$ . ■ ■

It is obvious that determining whether  $\left( F|_{X_i=1(0)} - F|_{X_i=0(1)} \right) \geq 0$  is the same as determining whether  $\left( F|_{X_i=1(0)} - F|_{X_i=0(1)} \right)$  is a probability expression.

Example 2.20: Consider the function  $f = \bar{x}_1 x_3 \vee x_2 \bar{x}_3$

$$\begin{aligned} F &= (1 - X_1)X_3 + X_2(1 - X_3) \\ &= X_3 - X_1X_3 + X_2 - X_2X_3. \end{aligned}$$

$$(1) \quad F|_{X_1=1} = X_3 - X_3 + X_2 - X_2 X_3 = X_2 - X_2 X_3$$

$$F|_{X_1=0} = X_3 + X_2 - X_2 X_3.$$

Since  $F|_{X_1=0} - F|_{X_1=1} = X_3$  which is a probability expression for  $x_3$ , therefore  $f$  is negative in  $x_1$ .

$$(2) \quad F|_{X_2=1} = X_3 - X_1 X_3 + 1 - X_3 = 1 - X_1 X_3$$

$$F|_{X_2=0} = X_3 - X_1 X_3.$$

$F|_{X_2=1} - F|_{X_2=0} = 1 - X_3$  which is a probability expression for  $\bar{x}_3$ . Hence  $f$  is positive in the variable  $x_2$ .

$$(3) \quad F|_{X_3=1} = 1 - X_1 + X_2 - X_2 = 1 - X_1$$

$$F|_{X_3=0} = X_2.$$

Since neither  $F|_{X_3=1} - F|_{X_3=0}$  nor  $F|_{X_3=0} - F|_{X_3=1}$  correspond to a probability expression,  $f$  is neither positive nor negative in  $x_3$ .

## 2.7 Concluding Remarks

The main contribution in this chapter is the identification and construction of a recursively defined matrix  $P$  with the property that the spectrum  $S$  (an equivalent representation for the probability expression  $F$ ) is given by

$S = AP$  where  $A$  is the minterm vector of the function  $f$ . The elegant structure of  $P$  is helpful in identifying useful properties of  $P$ ,  $S$  and  $F$ .

The analysis presented in this chapter yields an insight into the relationships between the spectrum  $S$ , the RMC coefficient vector  $a$ , and the Walsh coefficient vector  $C$  of a Boolean function  $f$ . It has also been shown that the computational complexity of obtaining  $a$  from  $S$  is less than the complexity of obtaining  $S$  from  $a$ .

## CHAPTER 3

### TEST GENERATION FOR COMBINATIONAL CIRCUITS

#### 3.1 Introduction

A theory of developing probability expressions for Boolean functions was developed in Chapter 2. In this chapter we shall study the application of probability expressions to the problem of test generation for digital circuits.

Testing digital circuits consists of applying a sequence of input patterns to a circuit, observing the output sequence, and comparing it with a precomputed normal response. In the absence of discrepancy between the observed and expected responses, the circuit passes the test and is said to function correctly. Otherwise, there exists a physical fault in the circuit and further diagnosis may be carried out until the fault is isolated to the desired level of accuracy.

Physical faults are often modeled as logical faults in generating tests. This facilitates fault analysis considerably. In Sections 3.3 and 3.4 of this chapter, we shall be dealing with the stuck line fault model. This means we will study physical faults for which logic signals appear



to be stuck at (invariant at) a logical value 0 or 1. Faults may be single or multiple depending upon the number of faults that can be simultaneously present in the circuit. Our analysis is restricted to the single fault model.

Many algorithms have been presented for test generation in digital circuits. These algorithms make use of algebraic (or equational), topological, or functional descriptions of the circuits under consideration. These test generation algorithms can be divided into two classes which will be referred to as Deterministic and Random test generation techniques.

#### Deterministic Test Generation Algorithms

The central concept in these algorithms is to sensitize a path deterministically and thereby propagate fault effects present along the path to outputs or other observable points. An input pattern is a "test" for a fault when the response of the normal and faulty circuits are different for this input pattern.

The Boolean difference [SHB68], Poage's procedure [Po63] and the equivalent normal form [Ar66] are examples of deterministic test generation techniques. The D-algorithm [Ro66], formalized in terms of a cubical algebra, is an algorithm based on a gate level topological description of a circuit.



monitors

applying randomly

## Random Test Generation Algorithms

Digital circuits are often tested by applying randomly generated patterns to the unit under test (UUT).

In one method, a test pattern sequence  $T_1$  of length  $L$  is applied to a known good circuit and the UUT as shown in Figure 3.1. The output responses are compared and the circuit is considered "to be fault free" if no discrepancy is observed in the output responses. The test length  $L$  is a function of the desired level of effectiveness in testing the circuit.  $T_1$  is usually generated by a hardwired digital pattern generator.

In another method, the test pattern sequence  $T_2$  is usually processed through a minicomputer and applied to the UUT.  $T_2$  is again a randomly generated sequence. The expected response and a fault dictionary are determined by prior simulation of a software model of the circuit under test.

The effectiveness of applying random input patterns in testing a circuit has been previously studied [AA72, HB73, AA75a, Ra71]. The problem of determining the optimal input probabilities for generating "effective" patterns has also been studied [AA76].

In this chapter we will develop a deterministic test generation algorithm based on the partial differential of the probability expression  $F$  with respect to  $X_i$ , denoted by

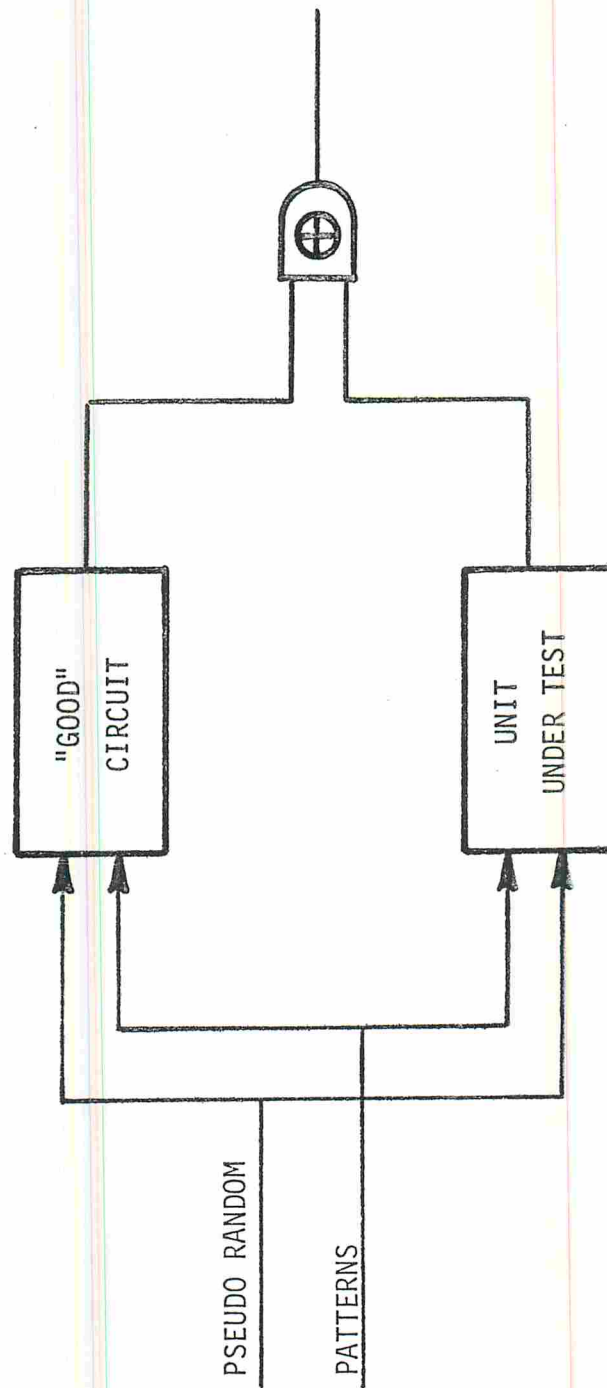


Figure 3.1. A method for testing digital circuits using pseudo-random patterns

$\frac{\partial F}{\partial X_i}$ . The relationship between  $\frac{\partial F}{\partial X_i}$  and the Boolean difference of function  $f$  with respect to signal  $x_i$ , denoted by  $\frac{df}{dx_i}$ , is also studied. In addition, a random test generation procedure, also based on the use of  $\frac{\partial F}{\partial X_i}$ , is presented.

### 3.2 Probability Expressions and Differential Calculus

The concept of expressing switching functions as a real sum of partial products of uncomplemented variables using the identities

$$\bar{x} = 1 - x$$

$$x_1 \oplus x_2 = x_1 + x_2 - 2x_1x_2$$

$$x_1 \vee x_2 = x_1 + x_2 - x_1x_2$$

is discussed in [DDT78]. The real sum is denoted by  $f^r$  in [DDT78]. It seems that by using an additional identity  $x_1 \wedge x_2 = x_1x_2$ , replacing  $x_i$  by  $X_i$  in  $f^r$ , and performing exponent suppression on the resultant expression, one obtains a probability expression for the function  $f$ . A detailed treatment of the real derivative of the real sum  $f^r$  is also presented in [DDT78].

We now present the basic definitions and theorems which will be used in subsequent sections.

Definition 3.1: Let  $G(b_1, b_2, \dots, b_i, \dots, b_m)$  be a real func-

tion of the real variables  $b_1, b_2, \dots, b_m$  defined over the interval  $[I_1, I_2]$ . The partial differential of the function  $G$  with respect to the variable  $b_i$  is defined by

$$\frac{\partial G}{\partial b_i} = \lim_{\Delta b_i \rightarrow 0} \left\{ \frac{[G(b_1, b_2, \dots, b_{i-1}, b_i + \Delta b_i, b_{i+1}, \dots, b_m) - G(b_1, b_2, \dots, b_{i-1}, b_i, b_{i+1}, \dots, b_m)]}{\Delta b_i} \right\}.$$

Let  $F(X_1, X_2, \dots, X_n)$  be the probability expression for the Boolean function  $f(x_1, x_2, \dots, x_n)$ . Then we can write  $F = X_i F_1 + F_2$  where  $F_1$  and  $F_2$  are functions of the variables  $X_1, X_2, \dots, X_{i-1}, X_{i+1}, \dots, X_n$ .

$$\text{Hence } \frac{\partial F}{\partial X_i} = F_1.$$

Theorem 3.1:

$$\begin{aligned} \frac{\partial F}{\partial X_i} &= F(X_1, X_2, \dots, X_{i-1}, X_i=1, X_{i+1}, \dots, X_n) \\ &\quad - F(X_1, X_2, \dots, X_{i-1}, X_i=0, X_{i+1}, \dots, X_n). \end{aligned}$$

Proof: We know  $F = X_i F_1 + F_2$ . Hence

$$F(X_1, X_2, \dots, X_{i-1}, X_i=1, X_{i+1}, \dots, X_n) = F_1 + F_2$$

and

$$F(X_1, X_2, \dots, X_{i-1}, X_i=0, X_{i+1}, \dots, X_n) = F_2.$$

Hence,

$$F(X_1, X_2, \dots, X_i=1, \dots, X_n) - F(X_1, X_2, \dots, X_i=0, \dots, X_n) = F_1.$$



Since  $\frac{\partial F}{\partial X_i} = F_1$ , we have

$$\begin{aligned}\frac{\partial F}{\partial X_i} &= F(X_1, X_2, \dots, X_{i-1}, X_i=1, X_{i+1}, \dots, X_n) \\ &\quad - F(X_1, X_2, \dots, X_{i-1}, X_i=0, X_{i+1}, \dots, X_n) .\end{aligned}$$

Equation (5.35) in [DDT78] which states that  $\frac{\partial^r f^r}{\partial x_i} = f(x_i=1) - f(x_i=0)$  is analogous to Theorem 3.1.

We shall denote  $F(X_1, X_2, \dots, X_{i-1}, X_i=1(0), X_{i+1}, \dots, X_n)$  by  $F|_{X_i=1(0)}$  for subsequent discussions. It is also important to note that  $\frac{\partial F}{\partial X_i}$  is independent of the variable  $X_i$ .

Lemma 3.1: For  $X_j \in [0,1]$ ,  $j = 1, 2, \dots, i-1, i+1, \dots, n$ , the range of  $\frac{\partial F}{\partial X_i}$  is the interval  $[-1,1]$ .

Proof:  $\frac{\partial F}{\partial X_i} = F|_{X_i=1} - F|_{X_i=0}$ . But  $F|_{X_i=1(0)}$  is a probability expression and takes values from the interval  $[0,1]$  when  $X_j \in [0,1]$  for  $j = 1, 2, \dots, i-1, i+1, \dots, n$ . Hence  $\frac{\partial F}{\partial X_i}$  is in the interval  $[-1,1]$ .

Example 3.1: Consider the Boolean function  $f = x_1 x_2 \vee \bar{x}_2 x_3$  where  $F(X_1, X_2, X_3) = X_1 X_2 + X_3 - X_2 X_3$

$$F = X_2(X_1 - X_3) + X_3 .$$

By Definition 3.1

$$\begin{aligned}\frac{\partial F}{\partial X_2} &= \lim_{\Delta X_2 \rightarrow 0} \left\{ \frac{[(X_2 + \Delta X_2)(X_1 - X_3) + X_3] - [X_2(X_1 - X_3) + X_3]}{\Delta X_2} \right\} \\ &= X_1 - X_3\end{aligned}$$

$$F|_{X_2=1} = X_1 - X_3 + X_3 = X_1$$

$$F|_{X_2=0} = X_3$$

$$\frac{\partial F}{\partial X_2} = F|_{X_2=1} - F|_{X_2=0} = X_1 - X_3.$$

It can be seen that  $\frac{\partial F}{\partial X_2}$  assumes values in the interval  $[-1,1]$  when  $X_1, X_3 \in [0,1]$ .

The function  $\frac{\partial F}{\partial X_i}$  is a measure of the variation of  $F$  with respect to the variable  $X_i$ .  $\frac{\partial F}{\partial X_i} = 0$  implies that  $F$  does not vary with respect to the variable  $X_i$ .  $\frac{\partial F}{\partial X_i} > 0$  indicates that positive (negative) change in  $X_i$  results in positive (negative) change in  $F$ .  $\frac{\partial F}{\partial X_i} < 0$  indicates that positive (negative) change in the value of  $X_i$  result in negative (positive) change in  $F$ .

Example 3.2: We know from Example 3.1 that for  $F = X_1 X_2 + X_3 - X_2 X_3$ ,  $\frac{\partial F}{\partial X_2} = X_1 - X_3$

$$\left. \frac{\partial F}{\partial X_2} \right|_{X_1=0, X_3=0} = 0.$$

Hence the function  $F$  is invariant with respect to  $X_2$  when  $X_1 = X_3 = 0$ .

$$\left. \frac{\partial F}{\partial X_2} \right|_{X_1=1, X_3=0} = 1.$$

Here the function  $F$  varies linearly with the variable  $X_2$  when  $X_1 = 1$  and  $X_3 = 0$ .

### 3.3 Deterministic Test Generation

In this section we present a new theory and procedure for deterministic test generation in combinational digital circuits.

Lemma 3.2: For  $X_j \in \{0,1\}$  and  $j = 1, 2, \dots, i-1, i+1, \dots, n$

$$\frac{\partial F}{\partial X_i} \in \{0, 1, -1\}.$$

Proof:  $\frac{\partial F}{\partial X_i} = F|_{X_i=1} - F|_{X_i=0}$ . By Theorem 2.4 we know that  $F|_{X_i=1}$  and  $F|_{X_i=0}$  the probability expressions, take values from the set  $\{0,1\}$  when  $X_j \in \{0,1\}$ . ■ ■

Table 3.1 shows all possible values of  $\frac{\partial F}{\partial X_i}$ ,  $X_j \in \{0,1\}$

Table 3.1. Table Showing All Possible Values for  $\frac{\partial F}{\partial X_i}$ ,  $X_j \in \{0,1\}$ .

$F _{X_i=1}$	$F _{X_i=0}$	$\frac{\partial F}{\partial X_i}$
0	0	0
0	1	-1
1	1	0
1	0	1

Definition 3.2: Consider a Boolean function  $f(x_1, x_2, \dots, x_n)$ . The Boolean difference of  $f$  with respect to the variable  $x_i$  is denoted by

$$\begin{aligned} \frac{df}{dx_i} \triangleq & f(x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) \\ & \oplus f(x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n) \end{aligned}$$

and represents all the conditions under which the value of  $f$  is sensitive to the value of  $x_i$ .

It has been shown that the Boolean difference can be used in the generation of tests for digital circuits [SHB68]. Let  $C$  be a circuit that realizes the function  $f$ . Consider the fault  $x_i$  s-a-0 in  $C$ . Let  $f^*$  denote the function corresponding to the circuit  $C$  with the fault in it.

Then  $f^* = f(x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n) \triangleq f_i(0)$ . The set of tests which detect the fault  $x_i$  s-a-0 is given by

$$\begin{aligned} T = f \oplus f^* &= [x_i \cdot f_i(1) + \bar{x}_i f_i(0)] \oplus f_i(0) \\ &= x_i [f_i(1) \oplus f_i(0)] \\ &= x_i \cdot \frac{df}{dx_i} . \end{aligned}$$

Thus  $x_i \cdot \frac{df}{dx_i}$  represents the set of tests which detect the fault  $x_i$  s-a-0. Similarly, it can be shown that  $\bar{x}_i \cdot \frac{df}{dx_i}$  represents the set of tests for the fault  $x_i$  s-a-1.

An input vector  $(a_1, a_2, \dots, a_n)$ ,  $a_i \in \{0, 1\}$ ,  $\forall i \in \{1, 2, \dots, n\}$  is a test for the fault  $x_i$  s-a-0 if and only if the expression  $T$  evaluates to 1 under the assignment  $\{x_1=a_1, x_2=a_2, \dots, x_n=a_n\}$ .

Theorem 3.2: Let  $F(X_1, X_2, \dots, X_i, \dots, X_n)$  be the probability expression for the Boolean function  $f(x_1, x_2, \dots, x_i, \dots, x_n)$ .

For  $X_j \in \{0, 1\}$ ,  $j = 1, 2, \dots, i-1, i+1, \dots, n$   $\left(\frac{\partial F}{\partial X_i}\right)^2 = 1$  if and only if  $\frac{df}{dx_i} = 1$ .

Proof: 1. Assume  $\left(\frac{\partial F}{\partial X_i}\right)^2 = 1$ . Hence

$$\frac{\partial F}{\partial X_i} = \pm 1.$$

Since

$$\frac{\partial F}{\partial X_i} = F|_{X_i=1} - F|_{X_i=0}$$

we have

$$\text{Case (i): } F|_{X_i=1} = 1 \quad \text{and} \quad F|_{X_i=0} = 0.$$

This implies that

$$f(x_1, x_2, \dots, x_i=1, \dots, x_n) = 1$$

and

$$f(x_1, x_2, \dots, x_i=0, \dots, x_n) = 0.$$

Hence



$$\begin{aligned}\frac{df}{dx_i} &= f(x_1, \dots, x_i=1, \dots, x_n) \oplus f(x_1, \dots, x_i=0, \dots, x_n) \\ &= 1.\end{aligned}$$

Case (ii):  $F|_{X_i=1} = 0$  and  $F|_{X_i=0} = 1$ .

Hence

$$f(x_1, \dots, x_i=1, \dots, x_n) = 0$$

and

$$f(x_1, \dots, x_i=0, \dots, x_n) = 1$$

therefore

$$\frac{df}{dx_i} = 1.$$

2. Assume  $\frac{df}{dx_i} = 1$ .

Case (i):  $f(x_1, \dots, x_i=1, \dots, x_n) = 1$

and

$$f(x_1, \dots, x_i=0, \dots, x_n) = 0.$$

Hence

$$F|_{X_i=1} = 1 \text{ and } F|_{X_i=0} = 0$$

and

$$\left(\frac{\partial F}{\partial X_i}\right)^2 = \left(F|_{X_i=1} - F|_{X_i=0}\right)^2 = 1.$$

Case (ii):  $f(x_1, \dots, x_i=1, \dots, x_n) = 0$

and

$$f(x_1, \dots, x_i=0, \dots, x_n) = 1.$$

Hence

$$F|_{X_i=1} = 0 \quad \text{and} \quad F|_{X_i=0} = 1$$

and

$$\left(\frac{\partial F}{\partial X_i}\right)^2 = (-1)^2 = 1.$$

■ ■

Equation (5.36) in [DDT78] which states that  $\left(\frac{\partial^r f}{\partial x_i}\right)^2 = \frac{\partial f}{\partial x_i}$  is analogous to Theorem 3.2.

The above theorem implies that  $\left(\frac{\partial F}{\partial X_i}\right)^2$  represents all the conditions under which the value of  $f$  is sensitive to  $x_i$ . An assignment to the variables  $X_j \in \{0,1\}$ ,  $j = 1,2,\dots, i-1,i+1,\dots,n$  that causes  $\frac{\partial F}{\partial X_i}$  to equal  $+1$  or  $-1$  represents one condition under which the value of the Boolean function  $f$  is sensitive to the value of  $x_i$ .

Example 3.3: Consider the function  $f = x_1 x_2 \vee \bar{x}_2 x_3$  of Figure 3.2.

$$\frac{df}{dx_2} = x_3 \oplus x_1$$

$$F = X_1 X_2 + X_3 - X_2 X_3$$

$$\frac{\partial F}{\partial X_2} = X_1 - X_3$$

$$\left(\frac{\partial F}{\partial X_2}\right)^2 = X_1^2 + X_3^2 - 2X_1 X_3.$$

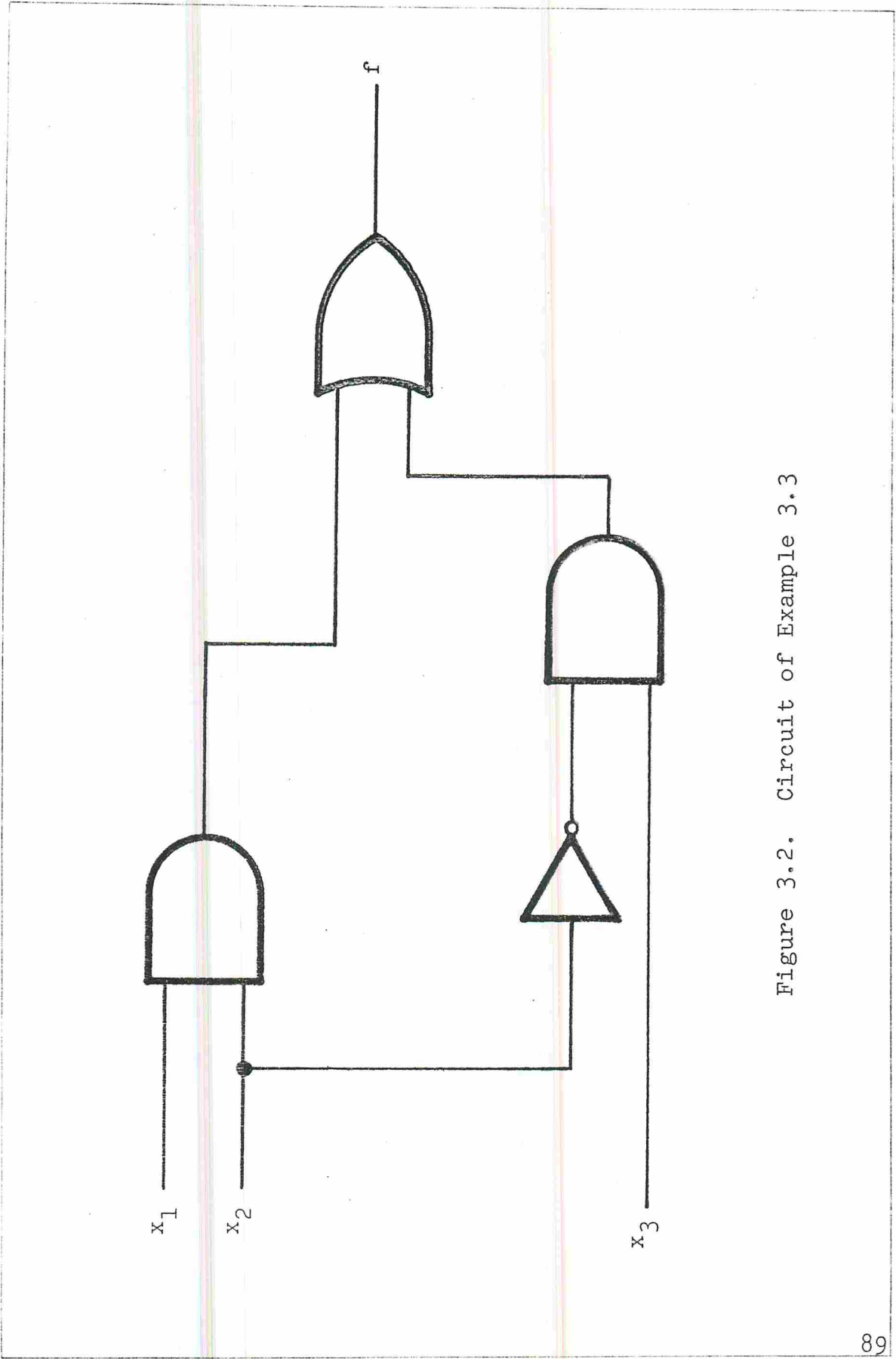


Figure 3.2. Circuit of Example 3.3

It is seen that  $\frac{df}{dx_2} = 1$  if and only if  $x_1 \oplus x_3 = 1$ , i.e., if  $x_1 = 0, x_3 = 1$  or  $x_1 = 1, x_3 = 0$ .

$$\left( \frac{\partial F}{\partial X_2} \right)^2 \Big|_{X_1=0, X_3=1} = 1$$

and

$$\left( \frac{\partial F}{\partial X_2} \right)^2 \Big|_{X_1=1, X_3=0} = 1.$$

It can be seen that

$$\frac{\partial F}{\partial X_2} \Big|_{X_1=0, X_3=1} = -1$$

and

$$\frac{\partial F}{\partial X_2} \Big|_{X_1=1, X_3=0} = 1.$$

Let  $e_i$  be an assignment vector which assigns binary values to a subset of  $\{x_1, x_2, \dots, x_{i-1}, x_{i+1}, \dots, x_n\}$ .  $f(x_1, x_2, \dots, x_n) \Big|_{e_i}$  denotes the evaluation of  $f(x_1, x_2, \dots, x_n)$  under assignment  $e_i$ .

Definition 3.3: The function  $f(x_1, x_2, \dots, x_i, \dots, x_n)$  is normally (inversely) sensitized with respect to the variable  $x_i$  and assignment  $e_i$  if

$$f(x_1, x_2, \dots, x_i, \dots, x_n) \Big|_{e_i} = x_i (\bar{x}_i).$$

Let  $E_i$  be an assignment vector which assigns binary values to a subset of  $\{X_1, X_2, \dots, X_{i-1}, X_{i+1}, \dots, X_n\}$  such that  $X_i = 1(0)$  if and only if  $x_i = 1(0)$  under assignment  $e_i$ .

Theorem 3.3:  $\frac{\partial F}{\partial X_i} \Big|_{E_i} = -1(1)$  if and only if the function  $f(x_1, x_2, \dots, x_i, \dots, x_n)$  is inversely (normally) sensitized with respect to the variable  $x_i$ .

Proof: (1) Let  $\frac{\partial F}{\partial X_i} \Big|_{E_i} = -1$ .

Hence

$$F \Big|_{X_i=1, E_i} = 0 \quad \text{and} \quad f(x_1, x_2, \dots, x_i=1, \dots, x_n) \Big|_{e_i} = 0 \quad (3.1)$$

$$F \Big|_{X_i=0, E_i} = 1 \quad \text{and} \quad f(x_1, x_2, \dots, x_i=0, \dots, x_n) \Big|_{e_i} = 1. \quad (3.2)$$

From (3.1) and (3.2)  $f(x_1, x_2, \dots, x_i, \dots, x_n) \Big|_{e_i} = \bar{x}_i$ .

(2) Assume  $f(x_1, x_2, \dots, x_i, \dots, x_n) \Big|_{e_i} = \bar{x}_i$ . Since  $f(x_1, x_2, \dots, x_i=0, \dots, x_n) \Big|_{e_i} = 1$

$$F \Big|_{X_i=0, E_i} = 1.$$

Also,  $f(x_1, x_2, \dots, x_i=1, \dots, x_n) \Big|_{e_i} = 0$ , and



$$F|_{X_i=1, E_i} = 0.$$

It follows that  $\left. \frac{\partial F}{\partial X_i} \right|_{E_i} = -1$ .

The second part of this theorem which states that  $\left. \frac{\partial F}{\partial X_i} \right|_{E_i} = 1$  if and only if  $f(x_1, x_2, \dots, x_i, \dots, x_n)$  is normally sensitized with respect to the variable  $x_i$ , follows in a similar fashion. ■ ■

Theorem 3.4:  $X_i \cdot \left( \frac{\partial F}{\partial X_i} \right)^2$  represents the expression for the set of all tests for the fault  $x_i$  s-a-0, and  $(1-X_i) \left( \frac{\partial F}{\partial X_i} \right)^2$  represents the set of all tests for the fault  $x_i$  s-a-1.

Proof: We know that  $x_i \cdot \frac{df}{dx_i}$  is the set of all tests for the fault  $x_i$  s-a-0 and  $\bar{x}_i \cdot \frac{df}{dx_i}$  is the set of all tests for the fault  $x_i$  s-a-1.

The theorem follows immediately from this fact and from Theorem 3.2. ■ ■

Example 3.4: Consider the circuit of Figure 3.3.

$$f = (x_2 \vee x_3)x_1 \vee \bar{x}_1 x_4$$

$$F = X_1(X_2 + X_3 - X_2 X_3) + X_4 - X_1 X_4.$$

We want to generate the set of tests for faults  $x_4$  s-a-1

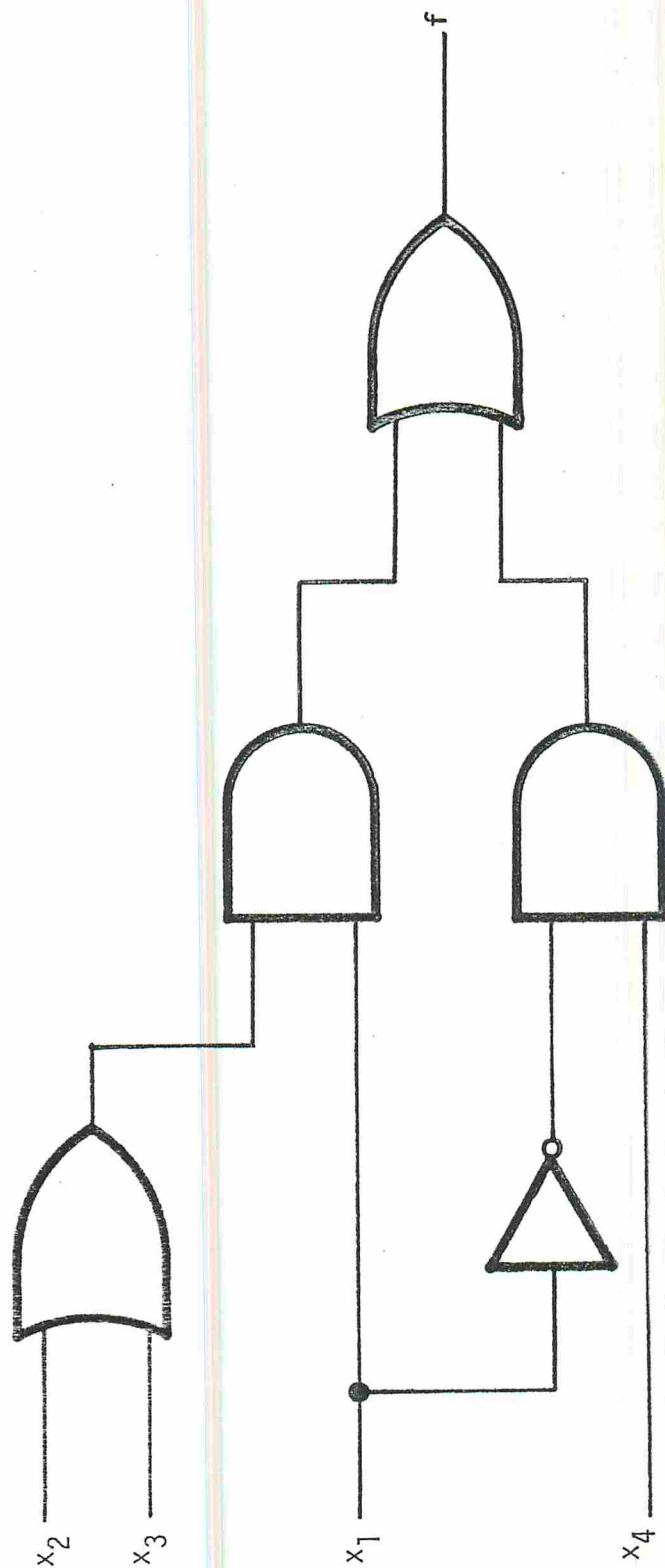


Figure 3.3. Circuit of Examples 3.4 and 3.11

and  $x_4$  s-a-0.

$$\begin{aligned}\frac{\partial F}{\partial X_4} &= F \Big|_{X_4=1} - F \Big|_{X_4=0} \\ &= [1-X_1+X_2(X_2+X_3-X_2X_3)] - [X_1(X_2+X_3-X_2X_3)] \\ &= (1-X_1).\end{aligned}$$

The set of tests which detect  $x_4$  s-a-0 is given by the expression  $X_4(1-X_1)^2$ . An input vector detects the fault when this expression evaluates to 1. Similarly the set of tests which detect  $x_4$  s-a-1 is given by the expression  $(1-X_4)(1-X_1)^2$ .

The Boolean difference method also yields the set of all tests that detect a fault. However, an explicit simulation of the circuit is needed to establish the response of the good (and the faulty) circuit for any test. This difficulty can be overcome by using a test generation scheme based on Theorem 3.3. Table 3.2 shows the value of output signals in a normal and a faulty circuit as a function of the expression  $\frac{\partial F}{\partial X_i}$ . We will use the symbol 0/1 to represent the logic signal having the value 0 in the normal circuit and 1 in the faulty circuit. It is clear that a test generation scheme based on Theorem 3.3 has an advantage over the Boolean difference in that we not only obtain the set of all tests for a given fault but also predict the behavior of the good and the faulty circuit without an actual simulation.

Table 3.2. Table Showing the Output Signal Values in Terms of the Input Signal Values and The Expression  $\frac{\partial F}{\partial X_i}$ .

INPUT VALUES FOR FAULT FREE AND FAULTY CIRCUITS

	$\frac{\partial F}{\partial X_i}$	1	-1
0/1	0/1	0/1	1/0
1/0	1/0	1/0	0/1

Theorem 3.5: Let  $C$  be a circuit which realizes  $f(x_1, x_2, \dots, x_n)$  and let  $h$  be an internal signal of  $C$ . Let  $f(x_1, x_2, \dots, x_n) = f'(x_1, x_2, \dots, x_n, h)$ . Then  $H \cdot \left(\frac{\partial F'}{\partial H}\right)^2$  represents the expression for the set of all tests detecting  $h$  s-a-0 and  $(1-H') \left(\frac{\partial F'}{\partial H}\right)^2$  represents the expression for the set of all tests detecting  $h$  s-a-1, where  $H$  is the probability expression for  $h$ .

Proof: We know that  $\left(\frac{\partial F'}{\partial H}\right)^2 = 1$  if and only if  $\frac{df}{dh} = 1$ , and  $H = 1$  if and only if  $h = 1$ . Since the set of tests for  $h$  s-a-0 is  $h \cdot \frac{df}{dh}$  and the set of tests for  $h$  s-a-1 is  $\bar{h} \cdot \frac{df}{dh}$ ,  $H \cdot \left(\frac{\partial F'}{\partial H}\right)^2$  is the expression for the set of all tests detecting  $h$  s-a-0 and  $(1-H) \left(\frac{\partial F'}{\partial H}\right)^2$  is the expression for the set of all tests detecting  $h$  s-a-1. ■ ■

Example 3.5: Consider the circuit of Figure 3.4. We will derive tests for the faults  $h$  s-a-0 and  $h$  s-a-1.

We can write  $f(x_1, x_2, x_3, x_4, h) = h \vee x_3 x_4$  where  $h = x_1 x_2$ .

$$F(X_1, X_2, X_3, X_4, H) = H + X_3 X_4 - H X_3 X_4$$

$$\frac{\partial F}{\partial H} = 1 - X_3 X_4.$$

The expression  $A_1 = H \left(\frac{\partial F}{\partial H}\right)^2 = X_1 X_2 (1 - X_3 X_4)^2$  represents the set of all tests which detect  $h$  s-a-0 and the expression  $A_2 = (1-H) \left(\frac{\partial F}{\partial H}\right)^2 = (1 - X_1 X_2) (1 - X_3 X_4)^2$  represents the set of all



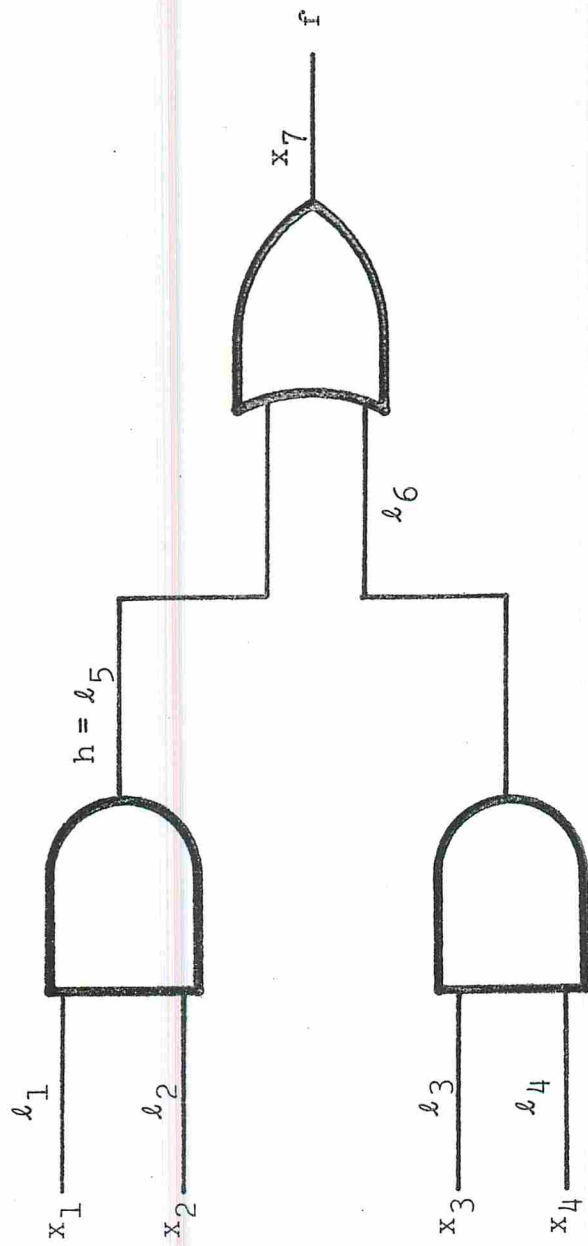


Figure 3.4. Circuit of Examples 3.5, 3.6, and 3.10

tests which detect h s-a-1. It should be noted that

$$A_1 + A_2 = \left( \frac{\partial F}{\partial h} \right)^2.$$

We now present two procedures for test generation in combinational circuits. The first procedure avoids the need for formal fault simulation and generates a near minimal test set.

Definition 3.4: A pseudo-Boolean (PB) function, is in general, a mapping  $f: B^n \rightarrow R$ ,  $B \in \{0,1\}$  from the set of real  $n$ -dimensional vertices  $\vec{v} = (v_1, v_2, \dots, v_n)$ ,  $v_j \in B$ ,  $j = 1, 2, \dots, n$  into the field of  $R$  of real numbers.

The problem of maximizing or minimizing a PB-function with or without constraints is known as pseudo-Boolean programming [HR68]. Several nonenumerative maximization algorithms are currently available [HR68, BE69, HP72] for pseudo-Boolean programming. The complexity of these procedures is of  $O(T)$  where  $T$  is the number of product terms in  $f$ .

Let  $l_1, l_2, \dots, l_p$  be all the logic signals of a circuit  $C$  realizing a Boolean function  $f(x_1, x_2, \dots, x_n)$ . The faults  $l_i$  s-a-0 and s-a-1 are represented by  $f_{2i-1}$  and  $f_{2i}$  respectively for  $i = 1, 2, \dots, p$ .

Let  $v_0$  denote the set  $\{f_1, f_2, \dots, f_{2p}\}$  and  $v_1$  denote

the collapsed<sup>2</sup> set of faults, hence  $v_1 \subseteq v_0$ .

Procedure 3.1: Test Generation for Combinational Circuits

1. For every line  $l_i$ , if

$$(f_{2i-1} \text{ or } f_{2i}) \in v_1$$

compute the expressions  $L_i = \Pr(l_i=1)$  and  $\frac{\partial F}{\partial L_i}$ ; if  $f_{2i-1} \in v_1$  then set  $T(f_{2i-1}) = L_i \left( \frac{\partial F}{\partial L_i} \right)^2$ , if  $f_{2i} \in v_1$  then set  $T(f_{2i}) = (1-L_i) \left( \frac{\partial F}{\partial L_i} \right)^2$ .

2. while  $v_1 \neq \{\phi\}$

1. compute  $S_1 = \sum_{f_k \in v_1} T(f_k)$
2. find  $V = (X'_1, X'_2, \dots, X'_n)$  using pseudo-Boolean programming, that maximizes  $S_1$  given that  $X'_k \in \{0,1\}$  for  $k=1,2,\dots,n$ .
3. determine  $D_1$ , the set of faults detected by  $V$ .
4.  $v_1 \leftarrow v_1 - D_1$

end while

Example 3.6: Consider the circuit shown in Figure 3.4.

<sup>2</sup>Faults  $\alpha, \beta$  are equivalent if and only if every test that detects  $\alpha$  also detects  $\beta$  and every test that detects  $\beta$  also detects  $\alpha$ . Equivalence fault collapsing in test generation consists of considering one fault from each set of equivalent faults.

$$v_0 = \{f_1, f_2, \dots, f_{14}\}$$

$$v_1 = \{f_1, f_2, f_4, f_5, f_6, f_8, f_{10}, f_{13}\}.$$

$$1. \quad T(f_1) = X_1 X_2 (1 - X_3 X_4)$$

$$T(f_2) = (1 - X_1) X_2 (1 - X_3 X_4)$$

$$T(f_4) = X_1 (1 - X_2) (1 - X_3 X_4)$$

$$T(f_5) = (1 - X_1 X_2) X_3 X_4$$

$$T(f_6) = (1 - X_1 X_2) (1 - X_3) X_4$$

$$T(f_8) = (1 - X_1 X_2) X_3 (1 - X_4)$$

$$T(f_{10}) = (1 - X_1 X_2) (1 - X_3 X_4)$$

$$T(f_{13}) = X_1 X_2 + X_3 X_4 - X_1 X_1 X_3 X_4.$$

$$2. \quad S_1 = \sum_{f_k \in v_1} T(f_k)$$

$$X_1 = 0, X_2 = 1, X_3 = 0 \text{ and } X_4 = 1 \text{ maximizes } S_1.$$

The faults detected are given by  $D_1 = \{f_2, f_6, f_{10}\}$

$$v_1 = \{f_1, f_4, f_5, f_8, f_{13}\}$$

$$S_1 = \sum_{f_k \in v_1} T(f_k)$$

$$X_1 = 0, X_2 = 1, X_3 = 1 \text{ and } X_4 = 1 \text{ maximizes } S_1.$$

The faults detected are given by  $D_1 = \{f_5, f_{13}\}$

$$v_1 = \{f_1, f_4, f_8\}$$

$$S_1 = \sum_{f_k \in v_1} (f_k)$$

$X_1 = 1, X_2 = 0, X_3 = 1$  and  $X_4 = 1$  maximizes  $S_1$ .

$$D_1 = \{f_4, f_8\}$$

$$v_1 = \{f_1\}$$

$X_1 = 1, X_2 = 1, X_3 = 0$  and  $X_4 = 0$  maximizes  $S_1$

$$v_1 = \{\phi\}.$$

Hence the test set  $\{0101, 0111, 1011, 1100\}$  is a complete, and in this case a minimal, test set for the circuit of Figure 3.4.

Two of the salient features of Procedure 3.1 are:

1. no formal fault simulation is required.
2. at each stage, we find a vertex  $V$  (equivalently a test) that detects the maximum number of faults as yet undetected. Hence we obtain a "near-minimal" detection test set.

We now present another procedure for test generation in combinational circuits. This procedure differs from Procedure 3.1 in that it uses a fault simulator.

#### Procedure 3.2:

1. Pick an untested (undetected) fault  $f_j$  on line  $l_i$ .

Compute  $L_i(X_1, X_2, \dots, X_n)$  and  $\frac{\partial F(X_1, X_2, \dots, X_n)}{\partial L_i}$ .



2. Let  $f_j$  represent the fault  $l_i$  s-a-0 (1). Using pseudo-Boolean programming, determine  $V = (X'_1, X'_2, \dots, X'_n)$  that satisfies  $\frac{\partial F}{\partial L_i} = 1$  or  $-1$ , under the constraint  $L_i(X_1, X_2, \dots, X_n) = 1$  (0). If  $V$  does not exist,  $f_j$  is not detectable, hence drop  $f_j$  from the set of untested faults and go to step 4.
3. If  $V$  exists,  $V$  is a test for  $f_j$ . Via fault simulation, determine all faults  $D_1$  as yet undetected, which are detected by  $V$ . Drop  $D_1$  from the set of untested faults.
4. If there are any remaining untested faults, go to step 1.

### 3.4 Random Test Generation

In this section we will review techniques for the analysis of logic circuits with faults when input signals are generated according to a given probability distribution. We shall also present techniques for generating expressions for the probability of detecting a fault. Finally a random test generation procedure is presented.

Parker [PM75b] has devised the following method for computing the probability of detecting a fault. Consider a function  $f(x_1, x_2, \dots, x_n)$ . For any single stuck-at fault, one could add another input  $y$  so that when  $y = 0$ , the circuit behaves normally and for  $y = 1$ , the circuit appears to

contain the specific fault. This produces a new function  $f'(x_1, x_2, \dots, x_n, y)$ . Consider the function  $f \oplus f'$ . The probability that  $[f(x_1, x_2, \dots, x_n) \oplus f'(x_1, x_2, \dots, x_n, y=1)] = 1$  represents the probability of detecting the fault.

Since  $f'(x_1, x_2, \dots, x_n, y=0) = f(x_1, x_2, \dots, x_n)$ ,  $f(x_1, x_2, \dots, x_n) \oplus f'(x_1, x_2, \dots, x_n, y=1)$  is the Boolean difference of  $f'$  with respect to  $y$ .

Theorem 3.6 [Ko77]: Let  $f_1(x_1, x_2, \dots, x_k, x_{k+1}, \dots, x_n)$  and  $f_2(x_1, x_2, \dots, x_k, x_{m+1}, \dots, x_p)$  be two Boolean functions with common variables  $x_1, x_2, \dots, x_k$ . Then  $\Pr(f_1 f_2 = 1) = \Pr(f_1 = 1) \cdot \Pr(f_2 = 1)$  with exponents suppressed.

Corollary 3.1:  $\Pr[(f_1 + f_2) = 1] = \Pr(f_1 = 1) + \Pr(f_2 = 1) - \Pr(f_1 = 1) \cdot \Pr(f_2 = 1)$  with exponents suppressed.

We will denote  $f(x_1, x_2, \dots, x_i=0, \dots, x_n)$  by  $f|_{x_i=0}$  and  $f(x_1, x_2, \dots, x_i=1, x_n)$  by  $f|_{x_i=1}$ . One should note that a probability expression for  $f(x_1, x_2, \dots, x_i=0, \dots, x_n)$  is  $F(X_1, X_2, \dots, X_i=0, \dots, X_n)$  and that for  $f(x_1, x_2, \dots, x_i=1, \dots, x_n)$  is  $F(X_1, X_2, \dots, X_i=1, \dots, X_n)$ .

Example 3.7: Let  $f = x_1 x_2 \vee x_2 x_3 \vee x_1 x_3$  and  $F = X_1 X_2 + X_2 X_3 + X_1 X_3 - 2X_1 X_2 X_3$ . The probability expression for  $f' = f(x_1=0, x_2, x_3)$  is given by  $F' = F|_{X_1=0} = X_2 X_3$  and the probability expression for  $f'' = f(x_1=1, x_2, x_3)$  is given by  $F''|_{X_1=1} = X_2 + X_3 - X_2 X_3$ .

Theorem 3.7: Consider the Boolean function  $f(x_1, x_2, \dots, x_n)$ .

The probability expression for  $\frac{df}{dx_i}$ , denoted by  $\Pr\left(\frac{df}{dx_i} = 1\right)$ ,

is  $F\Big|_{X_i=1} + F\Big|_{X_i=0} - 2F\Big|_{X_i=1} \cdot F\Big|_{X_i=0}$  with exponents suppressed.

Proof:  $\Pr\left(\frac{df}{dx_i} = 1\right) = \Pr[f(x_1, \dots, x_i=0, \dots, x_n) \oplus f(x_1, \dots, x_i=1, \dots, x_n) = 1]$ . Hence

$$\Pr\left(\frac{df}{dx_i} = 1\right) = \Pr\left[\left(f\Big|_{x_i=0} \cdot \bar{f}\Big|_{x_i=1} + \bar{f}\Big|_{x_i=0} \cdot f\Big|_{x_i=1}\right) = 1\right].$$

Since the terms  $f\Big|_{x_i=0} \cdot \bar{f}\Big|_{x_i=1}$  and  $\bar{f}\Big|_{x_i=0} \cdot f\Big|_{x_i=1}$  are mutually exclusive, we have

$$\Pr\left(\frac{df}{dx_i} = 1\right) = \Pr\left(f\Big|_{x_i=0} \cdot \bar{f}\Big|_{x_i=1} = 1\right) + \Pr\left(\bar{f}\Big|_{x_i=0} \cdot f\Big|_{x_i=1} = 1\right).$$

By Theorem 3.6

$$\Pr\left(f\Big|_{x_i=1} \cdot \bar{f}\Big|_{x_i=1} = 1\right) = \Pr\left(f\Big|_{x_i=0} = 1\right) \cdot \Pr\left(\bar{f}\Big|_{x_i=1} = 1\right),$$

with exponents suppressed. Since  $\Pr\left(\bar{f}\Big|_{x_i=1} = 1\right) = 1 - \Pr\left(f\Big|_{x_i=1} = 0\right)$

we have

$$\Pr(f|_{x_i=0} \cdot \bar{f}|_{x_i=1} = 1) = \Pr(f|_{x_i=0} = 1) \left(1 - \Pr(f|_{x_i=1} = 1)\right)$$

with exponents suppressed

$$= (F|_{X_i=0}) (1 - F|_{X_i=1})$$

with exponents suppressed.

(3.3)

Similarly

$$\Pr(\bar{f}|_{x_i=0} \cdot f|_{x_i=1} = 1) = (1 - F|_{X_i=0}) (F|_{X_i=1}) \quad (3.4)$$

with exponents suppressed. Combining (3.3) and (3.4)

$$\Pr\left(\frac{df}{dx_i} = 1\right) = F|_{X_i=1} + F|_{X_i=0} - 2F|_{X_i=0} \cdot F|_{X_i=1}$$

with exponents suppressed. ■ ■

From Theorem 3.7, we can determine a value for the probability of sensitizing a path given the values of input signal probabilities. The following theorem will extend this concept to the probability of detecting a fault.

Theorem 3.8: The probability of detecting  $x_i$  s-a-0 is given by  $\Pr(x_i=1) \left( F|_{X_i=1} + F|_{X_i=0} - 2F|_{X_i=1} \cdot F|_{X_i=0} \right)$  with ex-

ponents suppressed and the probability of detecting  $x_i$  s-a-1 is given by

$$\left(1 - \Pr(x_i = 1)\right) \left(F \Big|_{X_i=1} {}^{+F} \Big|_{X_i=0} {}^{-2F} \Big|_{X_i=1} {}^{\cdot F} \Big|_{X_i=0}\right)$$

with exponents suppressed.

Proof: The probability of detecting  $x_i$  s-a-0 is given by

$$\Pr\left(x_i \cdot \frac{df}{dx_i} = 1\right) = \Pr(x_i = 1) \cdot \Pr\left(\frac{df}{dx_i} = 1\right).$$

But from Theorem 3.7 we know that

$$\Pr\left(\frac{df}{dx_i} = 1\right) = F \Big|_{X_i=1} {}^{+F} \Big|_{X_i=0} {}^{-2F} \Big|_{X_i=0} {}^{\cdot F} \Big|_{X_i=1}$$

with exponents suppressed.

Hence

$$\Pr\left(x_i \frac{df}{dx_i} = 1\right) = \Pr(x_i = 1) \left(F \Big|_{X_i=1} {}^{+F} \Big|_{X_i=0} {}^{-2F} \Big|_{X_i=1} {}^{\cdot F} \Big|_{X_i=0}\right)$$

with exponents suppressed.

Similarly we can derive the expression for the probability of detecting the fault  $x_i$  s-a-1. ■ ■

We know that the expression  $F \Big|_{X_i=1} {}^{+F} \Big|_{X_i=0} {}^{-2F} \Big|_{X_i=1} {}^{\cdot F} \Big|_{X_i=0}$  is independent of the variable  $X_i$  and hence there



will be no exponent suppression involved while taking the product of two terms  $\Pr[x_i=1]$  and  $\left[ F \Big|_{x_i=1} + F \Big|_{x_i=0} - 2F \Big|_{x_i=1} \cdot F \Big|_{x_i=0} \right]$ .

Example 3.8: Consider the circuit of Figure 3.3. We would like to derive the probability expression for detecting the faults  $x_1$  s-a-0 and  $x_1$  s-a-1.

$$f = x_1(x_2 \vee x_3) \vee \bar{x}_1 x_4$$

and

$$F = X_1(X_2 + X_3 - X_2 X_3) + (1 - X_1)X_4$$

$$F \Big|_{X_1=0} = X_4$$

$$F \Big|_{X_1=1} = X_2 + X_3 - X_2 X_3$$

$$2F \Big|_{X_1=0} F \Big|_{X_1=1} = 2X_4(X_2 + X_3 - X_2 X_3).$$

Hence

$$\begin{aligned} \Pr \left[ \frac{df}{dx_1} = 1 \right] &= F \Big|_{X_1=0} + F \Big|_{X_1=1} - 2F \Big|_{X_1=0} \cdot F \Big|_{X_1=1} \\ &= X_4 + X_2 + X_3 - X_2 X_3 - 2X_2 X_4 - 2X_2 X_3 + 2X_2 X_3 X_4 \end{aligned}$$

$$\begin{aligned} \Pr(\text{detecting } x_1 \text{ s-a-0}) &= X_1(X_4 + X_2 + X_3 - X_2 X_3 - 2X_2 X_4 - 2X_2 X_3 \\ &\quad + 2X_2 X_3 X_4) \end{aligned}$$

and

$$\begin{aligned} \Pr(\text{detecting } x_1 \text{ s-a-1}) &= (1-X_1)(X_4+X_2+X_3-X_2X_3-2X_2X_4 \\ &\quad - 2X_2X_3+2X_2X_3X_4) . \end{aligned}$$

Theorem 3.9: Let  $C$  be a circuit which realizes  $f(x_1, x_2, \dots, x_n)$  and let  $h$  be an internal signal of  $C$ . Let  $f(x_1, x_2, \dots, x_n) = f'(x_1, x_2, \dots, x_n, h)$  and  $H = \Pr(h=1)$ . Then the probability of detecting  $h$  s-a-0 is given by  $H \left( F' \Big|_{H=0} + F' \Big|_{H=1} - 2F' \Big|_{H=0} F' \Big|_{H=1} \right)$  with exponents suppressed and the probability of detecting  $h$  s-a-1 is given by  $(1-H) \left( F' \Big|_{H=0} + F' \Big|_{H=1} - 2F' \Big|_{H=0} F' \Big|_{H=1} \right)$  with exponents suppressed.

Proof: Similar to the proof of Theorem 3.5. ■ ■

We have previously established that  $\Pr\left(\frac{df}{dx_1} = 1\right)$  is given by  $F \Big|_{X_1=1} + F \Big|_{X_1=0} - 2F \Big|_{X_1=1} F \Big|_{X_1=0}$  with exponent suppression.

Theorem 3.10: For  $X_j \in [0,1]$ ,  $j = 1, 2, \dots, i-1, i+1, \dots, n$

$$\left( \frac{\partial F}{\partial X_i} \right)^2 \Big|_{\text{exponents suppressed}} = \Pr\left(\frac{df}{dx_i} = 1\right) .$$

Proof: 
$$\left( \frac{\partial F}{\partial X_i} \right)^2 = \left( F \Big|_{X_i=1} - F \Big|_{X_i=0} \right)^2$$

$$= \left( F \Big|_{X_i=1} \right)^2 + \left( F \Big|_{X_i=0} \right)^2 - 2F \Big|_{X_i=1} \cdot F \Big|_{X_i=0} .$$

Hence

$$\left( \frac{\partial F}{\partial X_i} \right)^2 \Big|_{\substack{\text{exponents} \\ \text{suppressed}}} = F \Big|_{X_i=1} + F \Big|_{X_i=0} - 2F \Big|_{X_i=1} F \Big|_{X_i=0}$$

with exponents suppressed

$$= \Pr \left( \frac{df}{dx_i} = 1 \right) .$$

Theorem 3.10 can be easily extended to internal signals of a circuit under consideration. It is also obvious that

$$X_i \left( \frac{\partial F}{\partial X_i} \right)^2 \Big|_{\text{exponents suppressed}}$$

and

$$(1-X_i) \left( \frac{\partial F}{\partial X_i} \right)^2 \Big|_{\text{exponents suppressed}}$$

represent the probability expressions for detecting the faults  $x_i$  s-a-0 and  $x_i$  s-a-1 respectively.

Example 3.9: Consider the circuit of Figure 3.2 where  $f = x_1 x_2 \vee \bar{x}_2 x_3$  and  $F = X_1 X_2 + X_2 - X_2 X_3$

$$\frac{df}{dx_2} = f|_{x_2=0} \oplus f|_{x_2=1} = x_1 \oplus x_3$$

$$\frac{\partial F}{\partial X_2} = F|_{X_2=1} - F|_{X_2=0}$$

$$= (X_1 + X_3 - X_3) - X_3$$

$$= X_1 - X_3$$

$$\left( \frac{\partial F}{\partial X_2} \right)^2 \Big|_{\text{exponents suppressed}} = X_1 + X_3 - 2X_1X_3$$

which is the probability expression for  $\frac{df}{dx_2}$ .

With Theorems 3.8 and 3.9 we can compute the probability of detecting faults on input and internal lines of a circuit realizing Boolean function  $f$ .

Presently there exists no technique to determine the probability of distinguishing between two faults  $\alpha$  and  $\beta$ . To distinguish between two faults one must apply a vector which will detect fault  $\alpha$  but not fault  $\beta$  (or vice versa).

Theorem 3.11: Let  $C$  be the circuit realizing  $f(x_1, x_2, \dots, x_n)$ . Let  $\alpha, \beta$  be two faults in  $C$ . Let  $A$  be the probability expression for detecting  $\alpha$ , and  $B$  be the probability expression for detecting  $\beta$ . Then the Probability of Distin-

guishing between  $\alpha$  and  $\beta$  is given by  $A+B-2AB$  with exponents suppressed.

Proof: The probability of distinguishing between  $\alpha$  and  $\beta$  is  $PR_{\alpha|\beta} = \Pr(f_{\alpha} \oplus f_{\beta} = 1)$  where  $f_{\alpha}$ ,  $f_{\beta}$  are the faulty functions. Hence  $PR_{\alpha|\beta} = \Pr[(f \oplus f_{\alpha}) \oplus (f \oplus f_{\beta}) = 1]$ . Denoting  $f \oplus f_{\alpha}$  by  $f_1$  and  $f \oplus f_{\beta}$  by  $f_2$  we have

$$\begin{aligned} PR_{\alpha|\beta} &= \Pr[f_1 \oplus f_2 = 1] \\ &= \Pr(f_1=1) + \Pr(f_2=1) - 2\Pr(f_1=1)\Pr(f_2=1) \end{aligned}$$

with exponents suppressed.

Since  $A = \Pr(f_1=1)$  and  $B = \Pr(f_2=1)$  the result follows.

It can be seen from Theorem 3.11 that if both  $\alpha$  and  $\beta$  are faults in input lines, the entire computation can be done on  $F(X_1, X_2, \dots, X_n)$ .

If either of the faults is located on an internal line  $h$ , then  $F'(X_1, X_2, \dots, X_n, H)$  must be computed first. Here  $F'(X_1, X_2, \dots, X_n, H)$  is the probability expression for  $f'(x_1, x_2, \dots, x_n, h) = f(x_1, x_2, \dots, x_n)$ .

Example 3.10: Consider the circuit of Figure 3.4

$$f = x_1 x_2 \vee x_3 x_4$$

and



$$F = X_1 X_2 + X_3 X_4 - X_1 X_2 X_3 X_4 .$$

We want to find the probability of distinguishing between  $x_1$  s-a-0 and  $x_4$  s-a-1.

$$F|_{X_1=0} = X_3 X_4$$

$$F|_{X_1=1} = X_2 + X_3 X_4 - X_2 X_3 X_4$$

A = Probability of detecting  $x_1$  s-a-0

$$\begin{aligned} &= X_1 (\cancel{X_3 X_4} + \cancel{X_2 X_3 X_4} - \cancel{X_2 X_3 X_4} - \cancel{2X_2 X_3 X_4} - \cancel{2X_3 X_4} + \cancel{2X_2 X_3 X_4}) \\ &= X_1 (X_2 - X_2 X_3 X_4) \end{aligned}$$

B = Probability of detecting  $x_4$  s-a-1

$$F|_{X_4=0} = X_1 X_2$$

$$F|_{X_4=1} = X_1 X_2 + X_3 - X_1 X_2 X_3 .$$

B = Probability of detecting  $x_4$  s-a-1

$$\begin{aligned} &= (1-X_4) (\cancel{X_1 X_2} + \cancel{X_1 X_2} + \cancel{X_3} - \cancel{X_1 X_2 X_3} - \cancel{2X_1 X_2} \\ &\quad - \cancel{2X_1 X_2 X_3} + \cancel{2X_1 X_2 X_3}) \\ &= (1-X_4) (X_3 - X_1 X_2 X_3) . \end{aligned}$$

Probability of distinguishing between  $x_1$  s-a-0 and  $x_4$  s-a-1

=  $A + B - 2AB$  with exponents suppressed

$$\begin{aligned}
 &= X_1 X_2 - \cancel{X_1 X_2 X_3 X_4} + X_3 X_4 - \cancel{X_3 X_4 X_1 X_2} + \cancel{X_1 X_2 X_3 X_4} \\
 &\quad - 2(X_1 X_2)(1 - X_3 X_4)(1 - X_4)X_3(1 - X_1 X_2) \\
 &= X_1 X_2 - X_1 X_2 X_3 + X_3 X_4.
 \end{aligned}$$

It is interesting to note that given the probability expression  $PR_{\alpha|\beta}$ , the pseudo-Boolean programming technique can be used to generate a deterministic test which distinguishes between the two faults  $\alpha$  and  $\beta$ .

Figure 3.5 shows the relationship developed in Sections 3.2, 3.3, and 3.4.

#### Experimental Results in Random Test Generation

We now present procedures for constructing "optimal" random tests for digital circuits.

Let  $PD(f_i, N)$  denote the probability of detecting fault  $f_i$  in  $N$  patterns.

Definition 3.5: The average probability of detection  $PD_{avg}(N)$  of a set of faults  $f_1, f_2, \dots, f_p$  is given by

$$PD_{avg}(N) = \sum_{i=1}^p p_i \cdot PD(f_i, N)$$

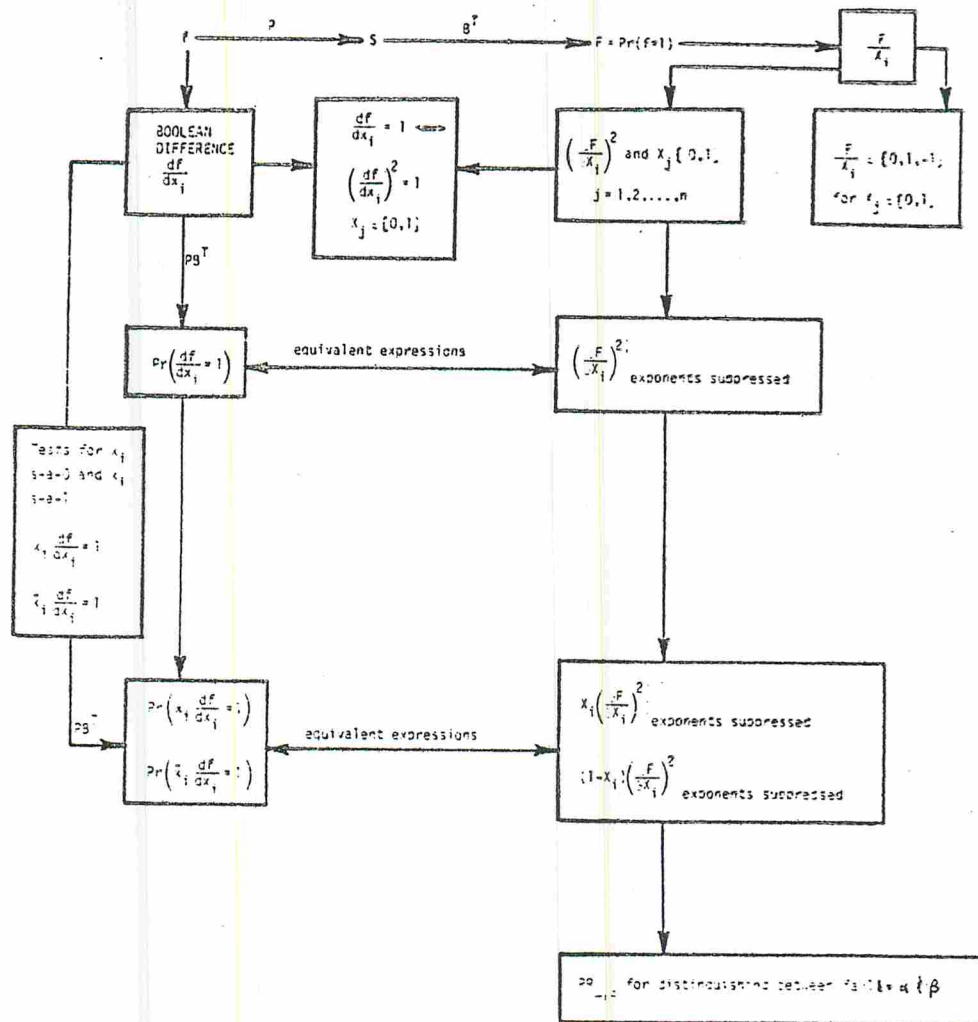


Figure 3.5. Summary of relationships developed in Sections 3.2, 3.3, and 3.4.1

where  $N$  is the number of applied patterns, and  $p_i$  is the probability of occurrence of  $f_i$ .

### Criterion for Optimality

The criterion for optimality is maximizing  $PD_{avg}(N)$ , or (equivalently) minimizing the average probability of non detection over the set of faults  $f_1, f_2, \dots, f_p$ , by the optimal choice of  $X_i$ ,  $i=1, 2, \dots, n$ . Under the assumption  $p_i = \frac{1}{p}$ , that is all faults are equally likely, we have

$$PD_{avg}(N) = \frac{1}{p} \sum_{i=1}^p PD(f_i, N).$$

Then  $p \cdot PD_{avg}(N) = \sum_i PD(f_i, N)$ .

In Chapter 5 we show that the product  $p \cdot PD_{avg}(N)$  is the expected number of faults detected in  $N$  patterns under the assumption  $p_i = \frac{1}{p}$ .

Procedure 3.3: Procedure for maximizing the average probability of detection over a set of faults  $\{f_i\}$ .

1. Compute the probability expressions for detecting faults  $f_i$ ,  $i=1, 2, \dots, p$ , using Theorems 3.8 and 3.9.
2. Let  $N$  be the number of patterns to be applied. The probability of detecting  $f_i$  in  $N$  patterns is  $PD(f_i, N) = 1 - (1 - \text{Probability of Detecting } f_i)^N$ .

$$3. \quad \beta = \sum_i PD(f_i, N). \quad (3.5)$$

4. Maximize  $\beta$  under the constraints  $0 \leq X_j \leq 1$  where  $X_j = \Pr(x_j=1)$ ,  $j = 1, 2, \dots, n$ .

It can be seen that the maximization of Eq.(3.5) is a nonlinear optimization problem with linear constraints. To obtain a solution, numerical procedures are required. We investigated two procedures for calculating the optimal input probability distribution for a given  $N$ .

#### Procedure A. Uniform Fine Grid Search

In this method the entire search space is uniformly divided into a fine grid. The value of the function  $\beta(X_1, X_2, \dots, X_n; N)$  is determined at all the points on the grid (note that there are only a finite number of points on the grid, but an infinite number of points in the search space). The maximum value of  $\beta$  and the associated input probabilities  $X_1, X_2, \dots, X_n$  on the grid points can be easily computed. This approach is computationally feasible when the number of input variables is small.

#### Procedure B. Variable Metric Method

The constrained nonlinear maximization problem given by Eq.(3.5) is equivalent to a minimization problem of the form



$$\text{minimize } p-\beta \text{ under the constraints } 0 \leq X_j \leq 1 \quad (3.6)$$

by determining the optimal values of  $X_j$ ,  $j = 1, 2, \dots, n$ .

Both of these problems can be converted to an unconstrained optimization problem by the transformation  $X_j = \sin^2 \theta_j$ ,  $j = 1, 2, \dots, n$ . We now have an unconstrained minimization problem of the form

$$\text{minimize } f(\underline{\theta}) = f(\theta_1, \theta_2, \dots, \theta_n).$$

It is convenient to express  $f(\underline{\theta})$  by a second order Taylor's series expansion about the point  $\underline{\theta}(k)$

$$\begin{aligned} f(\underline{\theta}(k+1)) &= f(\underline{\theta}(k)) + g^T(k) \Delta \underline{\theta}(k+1) + \frac{1}{2} [\Delta \underline{\theta}^T(k+1)] \\ &\quad \cdot G[\underline{\theta}(k) + \alpha \Delta \underline{\theta}(k+1)] \Delta \underline{\theta}(k+1) \quad 0 \leq \alpha \leq 1 \end{aligned}$$

where

$$\Delta \underline{\theta}(k+1) = \underline{\theta}(k+1) - \underline{\theta}(k), \quad g(k) = g(\underline{\theta}(k))$$

is the gradient of  $f(\underline{\theta})$  at  $\underline{\theta}(k)$ ,

and  $G(\underline{\theta}(k) + \alpha \Delta \underline{\theta}(k+1))$  is the Hessian matrix of the second partial derivatives evaluated at some point between  $\underline{\theta}(k)$  and  $\underline{\theta}(k+1)$ .

A necessary condition that a point  $\hat{\underline{\theta}}$  be a local minimum is  $g(\hat{\underline{\theta}}) = 0$ .

In the steepest descent method  $\Delta \underline{\theta}(k+1) = -\alpha_k g(k)$  and in the Newton-Raphson method

$$\Delta\theta(k+1) = -\alpha_k G^{-1}(\theta(k))g(k)$$

where  $\alpha_k$  is a scalar which determines the size of the step  $\Delta\theta(k+1)$ . The variable metric method is a balance between these methods. It involves a step of the form  $\Delta\theta(k+1) = -\alpha_k H_k g(k)$  where  $H_k$  is an approximation to  $G^{-1}(\theta(k))$ .

This approximation (often the identity matrix is used initially for  $H_0$  corresponding steepest descent method) is updated recursively at each step in a way that is intended to provide convergence to  $\hat{G}^{-1}$  as the sequence  $\theta(k)$  converges to  $\hat{\theta}$ .

Example 3.11: Consider the circuit of Figure 3.3. All s-a-0, s-a-1 faults in the circuit are assumed to be equally probable. We first present some results based on the uniform fine grid search. The grid size is set to 0.1. The maximum value of  $\beta = p \cdot PD_{avg}(N)$  and the associated optimal input probability distributions are shown in Table 3.3. In addition the minimum  $p \cdot PD_{avg}(N)$  and the corresponding worst case distributions are also shown. Other "close" solutions where

$$p \cdot PD_{avg}(N) \cong \text{Maximum } p \cdot PD_{avg}(N) - 0.05$$

are presented.  $p \cdot PD_{avg}(N)$  for the uniform distribution  $X_1 = X_2 = X_3 = X_4 = 0.5$  is also shown.

Table 3.3. Table Showing Input Distributions Corresponding to Maximum, Minimum  $p \cdot PD_{avg}$  and  $p \cdot PD_{avg}$  Corresponding to Uniform Distribution for Circuit of Example 3.11

Number of Patterns N	Type of Solution	$X_1$	$X_2$	$X_3$	$X_4$	$p \cdot PD_{avg}(N)$
2	optimal	0.7	0.2	0.1	1.0	11.7469
	optimal	0.7	0.1	0.2	1.0	11.7469
	"close"	0.7	0	0.2	1.0	11.7468
	"close"	0.7	0.2	0	1.0	11.7468
	"close"	0.7	0.3	0	1.0	11.7408
	"close"	0.7	0	0.3	1.0	11.7408
	"close"	0.6	0	0.2	1.0	11.7392
	"close"	0.6	0.2	0	1.0	11.7392
2	worst	1.0	1.0	1.0	0	2.00
2	uniform	0.5	0.5	0.5	0.5	9.332
6	optimal	0.6	0.3	0.2	0.8	17.9658
	optimal	0.6	0.2	0.3	0.8	17.9658
	"close"	0.6	0.2	0.2	0.9	17.9618
	"close"	0.6	0.2	0.2	0.8	17.9326
	"close"	0.6	0.2	0.3	0.9	17.9280
	"close"	0.6	0.3	0.2	0.9	17.9280
	"close"	0.6	0.1	0.3	0.9	17.9263
	"close"	0.6	0.3	0.1	0.9	17.9263
6	worst	1.0	1.0	1.0	0	2.00
6	uniform	0.5	0.5	0.5	0.5	16.504
10	optimal	0.6	0.3	0.3	0.7	20.0383
	"close"	0.6	0.3	0.3	0.6	20.0190
	"close"	0.5	0.3	0.3	0.6	19.9910
10	worst	1	1	1	0	2.0
10	uniform	0.5	0.5	0.5	0.5	19.062
14	optimal	0.6	0.3	0.3	0.6	20.9946
	"close"	0.6	0.3	0.4	0.6	20.9736
	"close"	0.6	0.4	0.3	0.6	20.9736
	"close"	0.5	0.3	0.3	0.6	20.9541
14	worst	1	1	1	0	2.0
14	uniform	0.5	0.5	0.5	0.5	

Table 3.4 has been constructed by first computing  $lp \cdot PD_{avg}(N)_J$  for all input probability distributions with grid size set to 0.1. Table 3.4 shows the number of input probability distributions yielding  $lp \cdot PD_{avg}(N)_J = 0, 1, \dots, 22$  for a given  $N$ . Table 3.5 shows the results obtained using the variable metric method and randomly chosen initial points. Figures 3.6a and 3.6b show the variation of  $\beta$  with respect to the variables  $X_3$  and  $X_4$ . The variables  $X_1$  and  $X_2$  have been fixed. It is clear from Figures 3.6a and 3.6b that the function  $\beta$  has numerous local maxima. The presence of many local maxima indicates that it is difficult to obtain a global maxima using the variable metric method.

Let  $\sigma(K)$  be the number of input distributions having  $[ \beta ] = lp \cdot PD_{avg}(N)_J = K$ . Figure 3.7 shows the relationship between  $K$  and  $\frac{\sigma(K)}{\mu}$  where  $\mu$  = total number of input probability distributions = 11<sup>4</sup>.  $\frac{\sigma(K)}{\mu}$  is essentially the probability that the expected number of faults detected equals  $K$ . Figure 3.8 and Figure 3.9 show  $\Omega_1(K)$  and  $\Omega_2(K)$ , the probability that the expected number of faults detected is greater than or equal to  $K$  and less than or equal to  $K$  respectively, for  $K = 0, 1, \dots, 22$ .

In the limiting case when  $N = \infty$ , it can be seen that  $\Omega_1(K) = 1$  for  $K = 0, 1, \dots, 22$ . Similarly when  $N = \infty$ ,  $\Omega_2(K) = 0$  for  $K = 0, 1, \dots, 21$  and  $\Omega_2(K) = 1$  for  $K = 22$ .



Table 3.4. Number of Input Distributions and Associated  $p \cdot PD_{avg}$  for Circuit of Example 3.11.

$\lfloor p \cdot PD_{avg}(N) \rfloor$	Number of Input Probability Distributions			
	N = 2	N = 6	N = 10	N = 14
0	0	0	0	0
1	0	0	0	0
2	29	17	15	13
3	106	10	8	8
4	363	61	46	24
5	856	282	227	226
6	1868	152	123	107
7	2569	389	133	71
8	3269	940	683	606
9	3753	818	474	288
10	1630	1233	636	470
11	198	1395	826	664
12	0	1843	1092	783
13	0	2321	1885	1684
14	0	2077	1784	1331
15	0	1541	1784	1716
16	0	1010	1601	1471
17	0	552	1386	1491
18	0	0	1266	1526
19	0	0	670	1460
20	0	0	2	702
21	0	0	0	0
22	0	0	0	0



Table 3.5. Table Showing the Result of the Variable Metric Method for the Circuit of Example 3.11

N	Initial Point ( $X_1, X_2, X_3, X_4$ )	$p \cdot PD_{avg}(N)$	Converging Point ( $X_1, X_2, X_3, X_4$ )	Number of Iterations	$p \cdot PD_{avg}(N)$
6	0.25, 0.25, 0.5, 0.5	16.055	0.31, 0.21, 0.45, 0.61	12	16.881
	0.5, 0.75, 0.5, 1	12.182	0.55, 0.65, 0.45, 0.92	15	13.821
	0.5, 0.5, 1, 0.75	12.878	0.57, 0.46, 0.92, 0.81	14	13.832

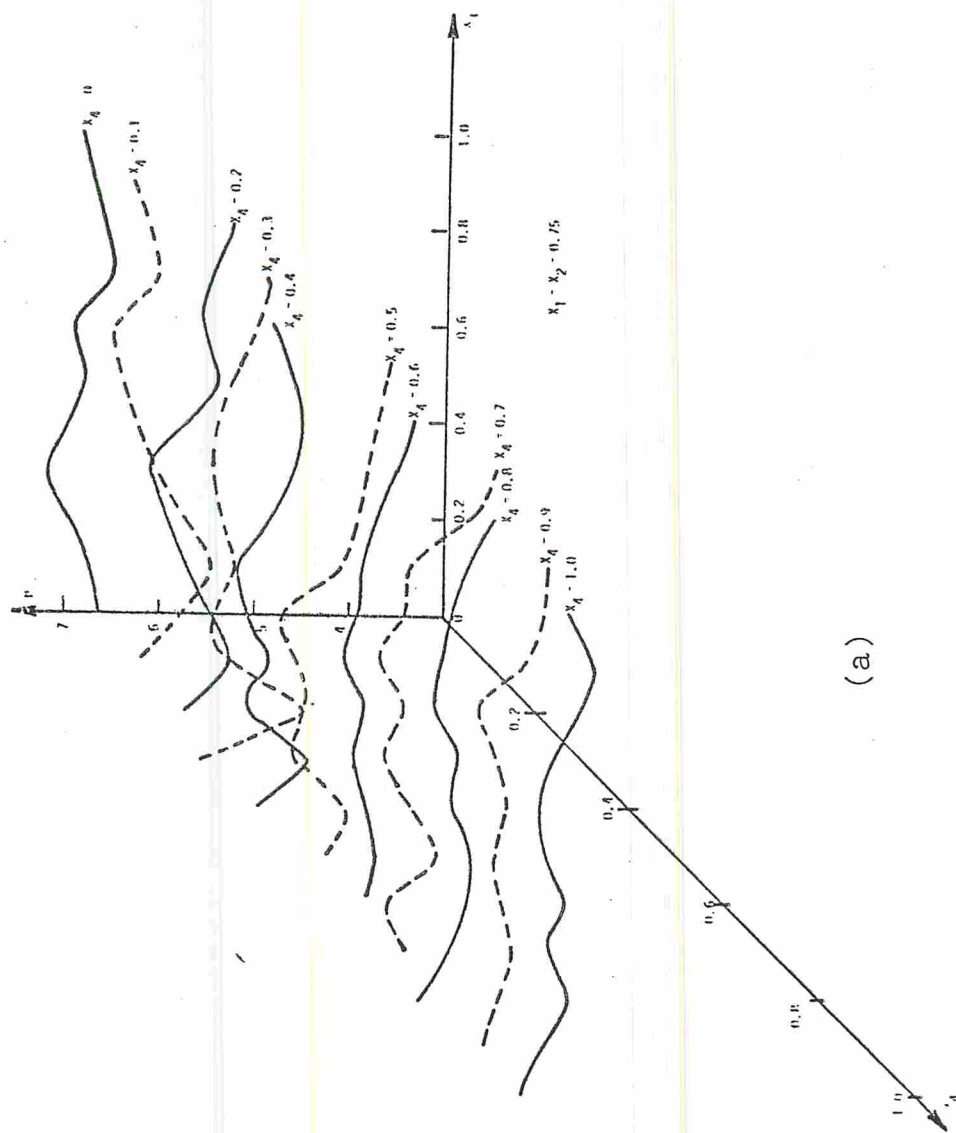


Figure 3.6. Variation of  $\beta = p \cdot \text{PD}_{\text{avg}}(N)$  with respect to variables  $X_3$  and  $X_4$

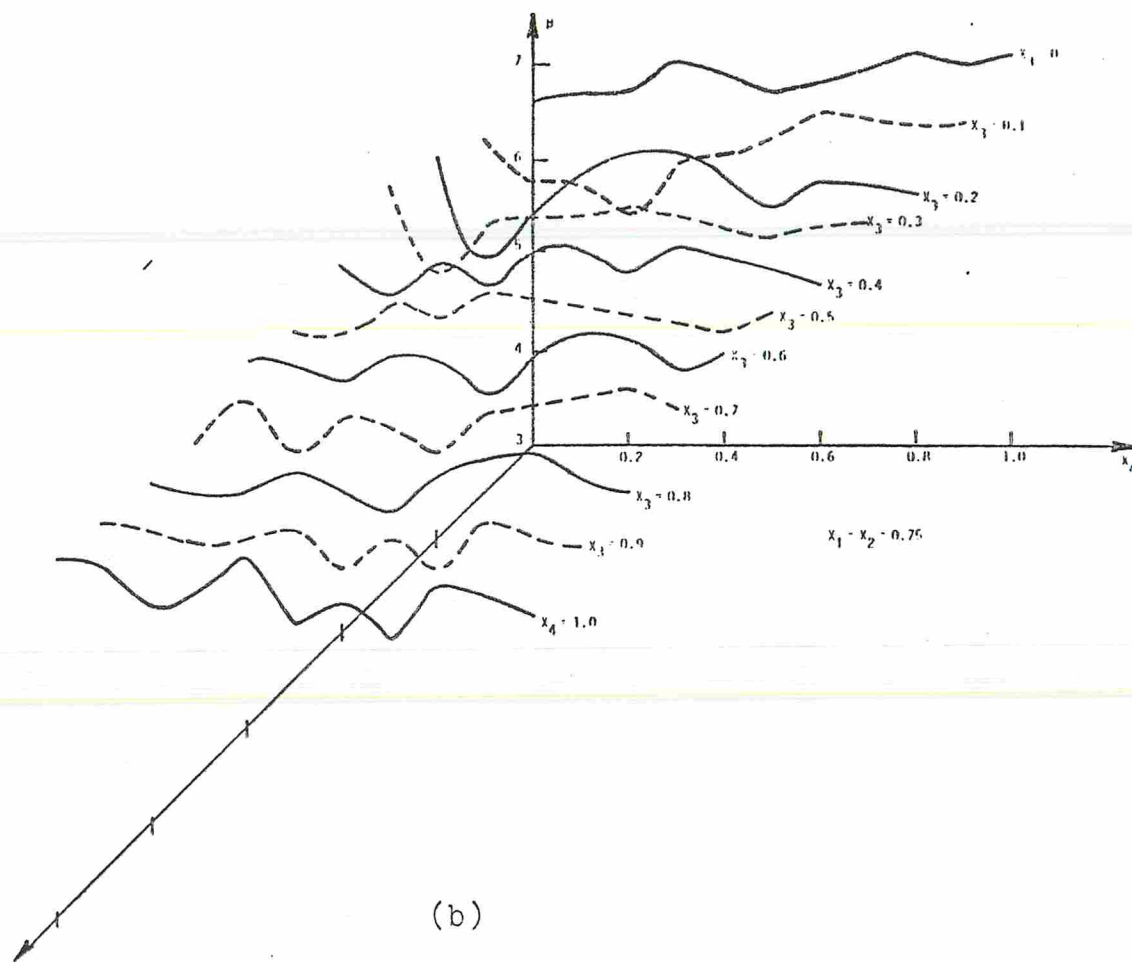


Figure 3.6. (Continued)

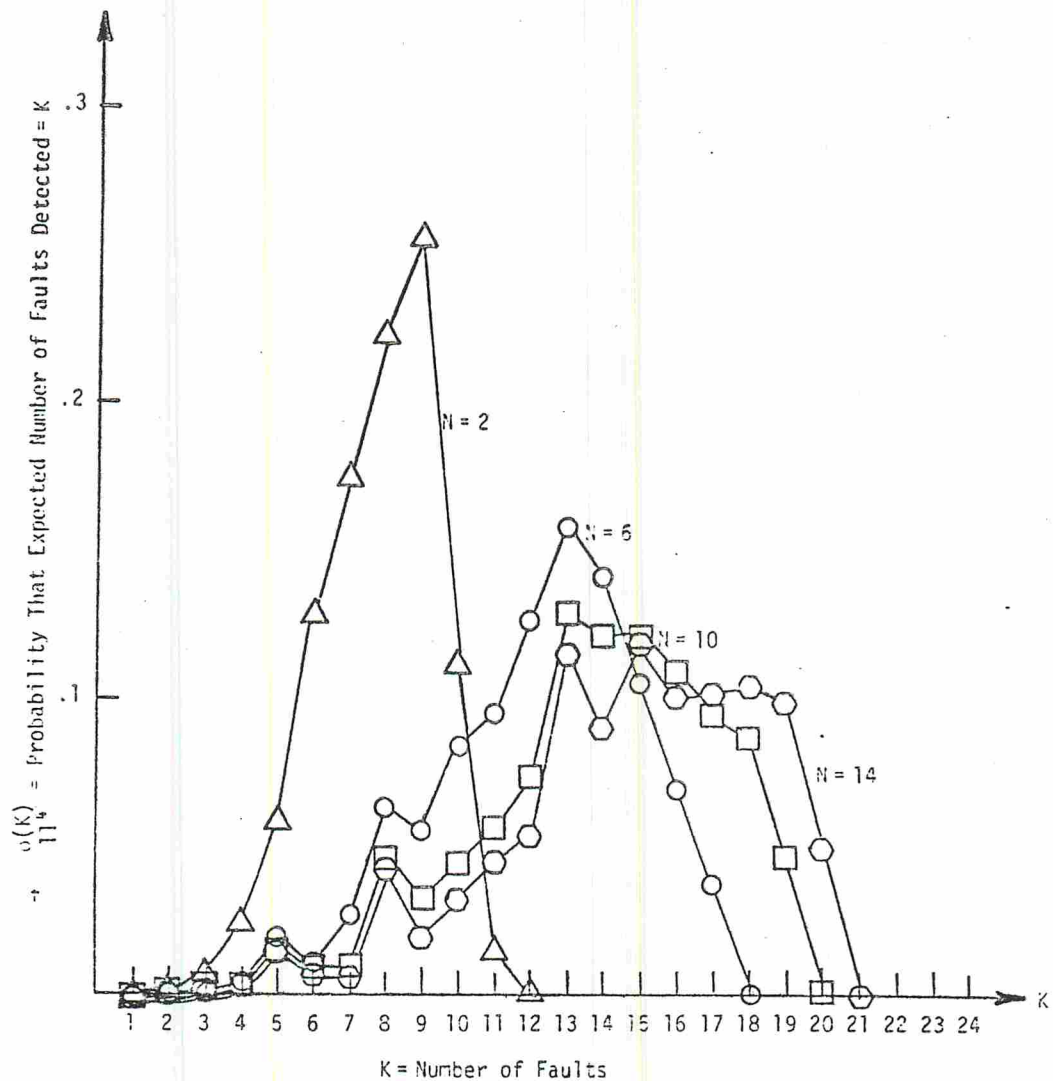


Figure 3.7. Relationship between K, the number of faults and the probability that the expected number of faults detected equals K, for different N, for the circuit of Example 3.11

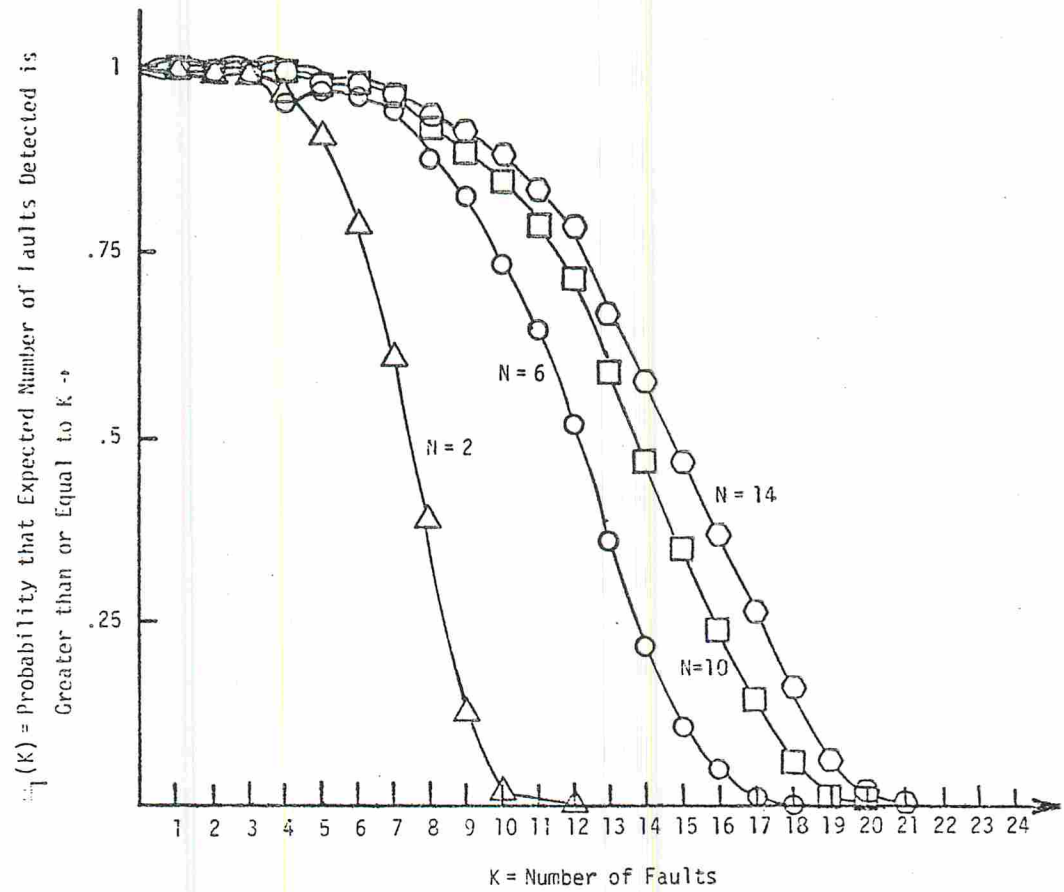


Figure 3.8. Relationship between  $K$ , the number of faults, and  $\Omega_1(K)$  for different  $N$  for the circuit of Example 3.11



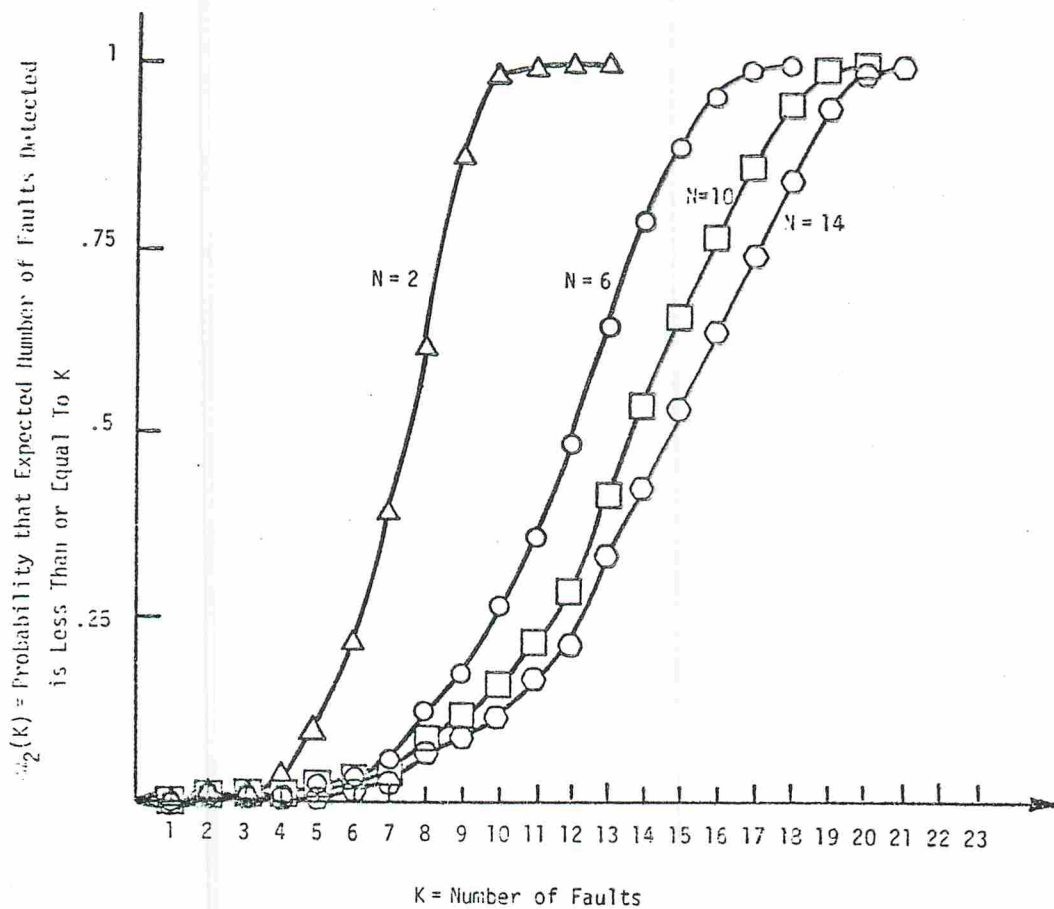


Figure 3.9. Relationship between  $K$ , the number of faults, and  $\Omega_2(K)$  for different  $N$  for the circuit of Example 3.11

Figure 3.10 shows the difference between maximum  $p \cdot PD_{avg}(N)$  and  $p \cdot PD_{avg}(N)$  for the uniform distribution as a function of  $N$ .

Example 3.12: Consider the circuit of Figure 3.11. All s-a-0 and s-a-1 faults are assumed to be equally probable.

Tables 3.6 and 3.7 show the results obtained using the uniform grid search procedure. The construction of Tables 3.6 and 3.7 is similar to that of Tables 3.3 and 3.4. Grid size is set to 0.1.

From these examples, the following observations can be made:

1. the maximum value of  $\beta(\underline{X}) = p \cdot PD_{avg}(N)(\underline{X})$  becomes less sensitive to  $\underline{X}$  as  $N$  increases.
2. the worst case distribution corresponds to the deterministic test which detects the least number of faults. Hence the minimum value of  $p \cdot PD_{avg}(N)$  and its associated input probability distribution remain unchanged for any  $N$ , since we apply the same deterministic test repeatedly.
3. let  $E(N)$  denote that the value of  $\lfloor p \cdot PD_{avg}(N) \rfloor$  for which there exists the maximum number of input probability distributions for a given  $N$ .  
 $E(N)$  is a non decreasing function of  $N$  (Fig.3.7).

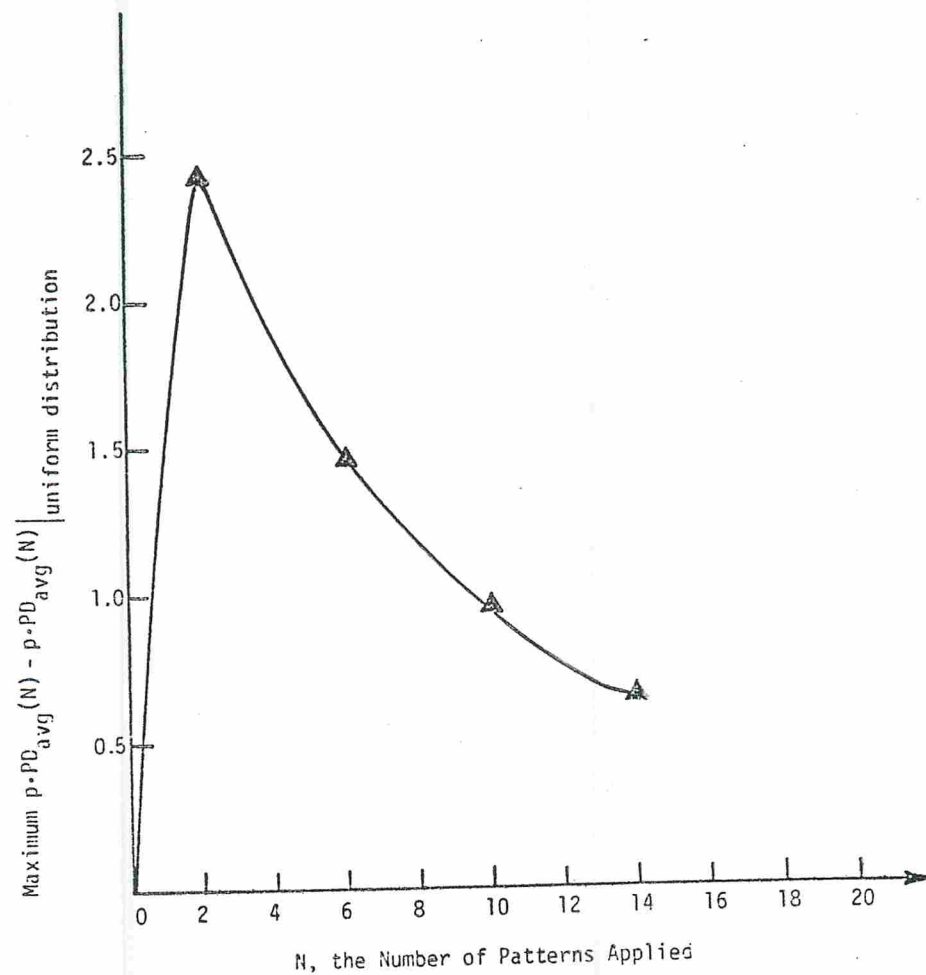


Figure 3.10.  $[ \text{Maximum } p \cdot PD_{avg}(N) - p \cdot PD_{avg}(N) | \text{uniform} ]$   
as a function of N  
distribution

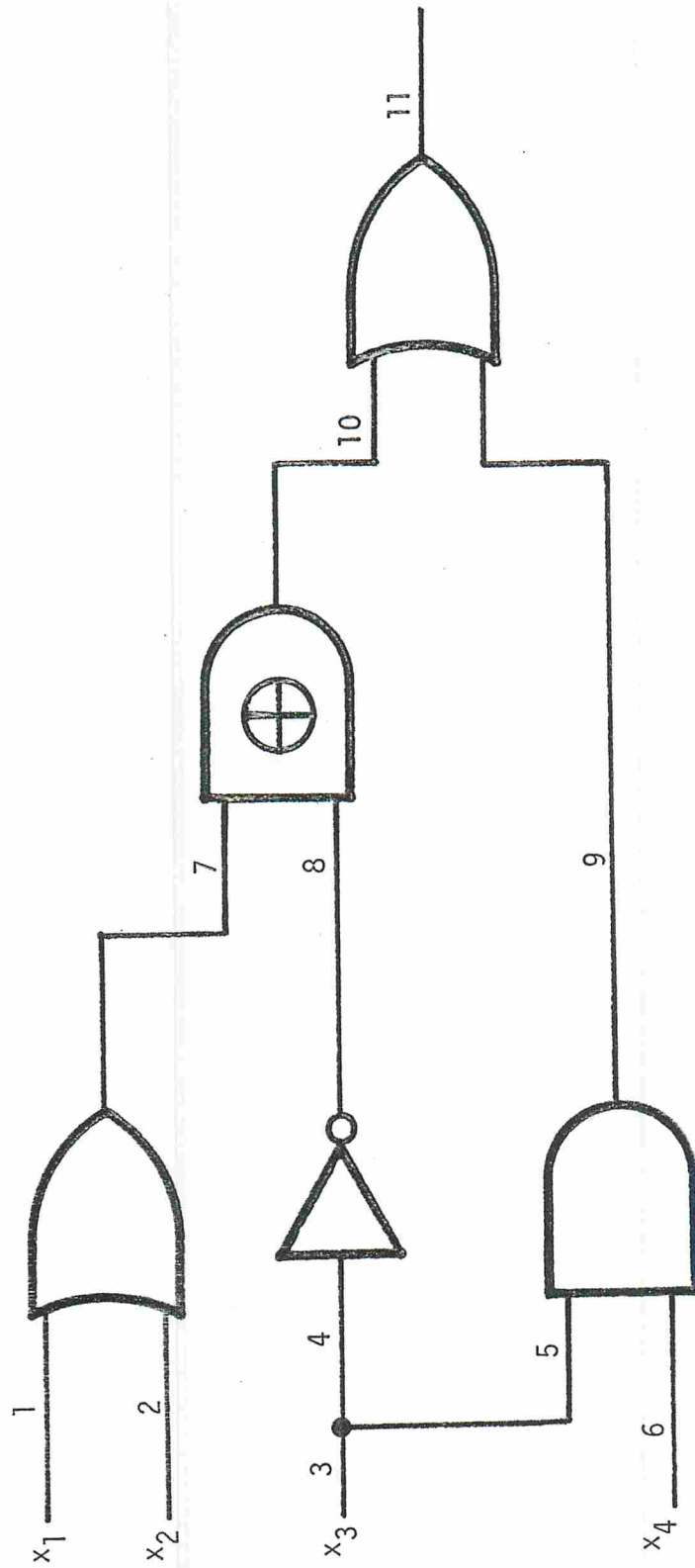


Figure 3.11. Circuit of Example 3.12

Table 3.6. Table Showing Various Input Probability Distributions and the Associated  $p \cdot PD_{avg}$  for Circuit of Example 3.12.

Number of Patterns N	Type of Solution	$X_1$	$X_2$	$X_4$	$X_4$	$p \cdot PD_{avg}(N)$
2	optimal	0	0.3	0.6	0	12.6356
	optimal	0.3	0	0.6	0	12.6356
	close	0.1	0.2	0.6	0	12.6292
	close	0.2	0.1	0.6	0	12.6292
	close	0.2	0.2	0.6	0	12.6250
	close	0.1	0.3	0.6	0	12.6203
	close	0.3	0.1	0.6	0	12.6203
	close	0	0.4	0.6	0	12.5984
	close	0.4	0	0.6	0	12.5984
	worst	0	1	1	1	2.000
	uniform	0.5	0.5	0.5	0.5	10.461
6	optimal	0.2	0.2	0.6	0.4	18.2520
	close	0.2	0.3	0.6	0.4	18.2368
	close	0.3	0.2	0.6	0.4	18.2368
	worst	0	1	1	1	2.0000
	uniform	0.5	0.5	0.5	0.5	16.893
10	optimal	0.3	0.2	0.6	0.5	20.2427
	optimal	0.2	0.3	0.6	0.5	20.2427
	close	0.3	0.3	0.6	0.5	20.2264
	close	0.2	0.2	0.6	0.5	20.2029
	worst	0	1	1	1	2.000
	uniform	0.5	0.5	0.5	0.5	18.995
14	optimal	0.3	0.3	0.6	0.6	21.1106
	close	0.3	0.3	0.6	0.5	21.0886
	close	0.3	0.2	0.6	0.6	21.0694
	close	0.2	0.3	0.6	0.6	21.0694
	close	0.2	0.3	0.6	0.5	21.0648
	close	0.3	0.2	0.6	0.5	21.0648
	worst	0	1	1	1	2.0000
	uniform	0.5	0.5	0.5	0.5	20.099



Table 3.7. Number of Input Distributions and Associated  $\lfloor p \cdot PD_{avg} \rfloor$  for Circuit of Example 3.12.

$\lfloor p \cdot PD_{avg}^{(N)} \rfloor$	Number of Input Probability Distributions			
	N = 2	N = 6	N = 10	N = 14
0	0	0	0	0
1	0	0	0	0
2	87	35	26	24
3	148	29	22	13
4	273	87	82	84
5	449	66	27	27
6	730	222	182	163
7	1097	172	104	72
8	2200	459	264	240
9	3608	499	199	122
10	3819	850	535	312
11	1882	1267	702	479
12	348	1817	1097	983
13	0	2092	1811	1669
14	0	2095	1504	1202
15	0	2030	1713	1213
16	0	1812	2011	1939
17	0	1048	1885	1934
18	0	61	1538	1706
19	0	0	892	1577
20	0	0	47	870
21	0	0	0	12
22	0	0	0	0

4. the difference between the maximum value of  $p \cdot PD_{avg}(N)$  and the value of  $p \cdot PD_{avg}(N)$  under the uniform distribution decreases with increasing  $N$ .
5. let  $p$  be the number of detectable faults in a circuit. The number of distributions which detect between  $\delta p$  and  $p$  faults, where  $0 < \delta < 1$ , increases with  $N$ .
6. the function  $\beta$  has numerous maxima as seen in Figures 3.6a and 3.6b.
7. the variable metric method yields little improvement over the initial probability distribution. This is due to the fact that there are numerous local maxima for the function  $\beta$ , and it is relatively flat.

### 3.5 Intermittent Failure Analysis

#### 3.5.1 Introduction

Intermittent failures can be defined as failures that change the normal function of circuits during randomly occurring intervals of time. An intermittent fault may therefore be present or absent at different intervals of time. Most of the faults occurring in digital systems are intermittent in nature [BH69]. A first order discrete parameter Markov model [Br73], a zero order Markov model [KP74, Sa77] and a continuous parameter Markov model [SKM79] have been used to analyze the behavior of intermittent faults.

In this section we present a model for introducing an intermittent fault into the circuit structure or description. This model enables the computation of probability expressions for circuit outputs in terms of the behavior of the intermittent fault under consideration.

### 3.5.2 Intermittent Fault Model

Consider the circuit of Figure 3.12. An intermittent fault can be modeled by introducing an input  $x_I$  such that the probability  $X_I = \Pr(x_I=1)$  is the probability that the intermittent fault is present. Note that in this model we can insert any expression for the probability  $X_I$ . We will be considering only intermittent faults which, when present, behave like permanent s-a-0 and s-a-1 faults. We will denote these intermittent faults by  $f_{I_0}$  and  $f_{I_1}$ .

The intermittent faults  $f_{I_1}$  (and  $f_{I_0}$ ) on line A in a circuit can be modeled as shown in Figures 3.13 (and 3.14).

Example 3.12: Consider the circuit in Figure 3.15. We will derive the probability expression for the output when the line  $x_1$  has the fault  $f_{I_1}$ . The modified circuit (which includes the effect of  $f_{I_1}$ ) is shown in Figure 3.16. The outputs of the original and modified circuits are denoted by  $f$  and  $f'$  respectively

$$F(X_1, X_2, X_3) = X_1 X_2 + X_3 (1 - X_2)$$

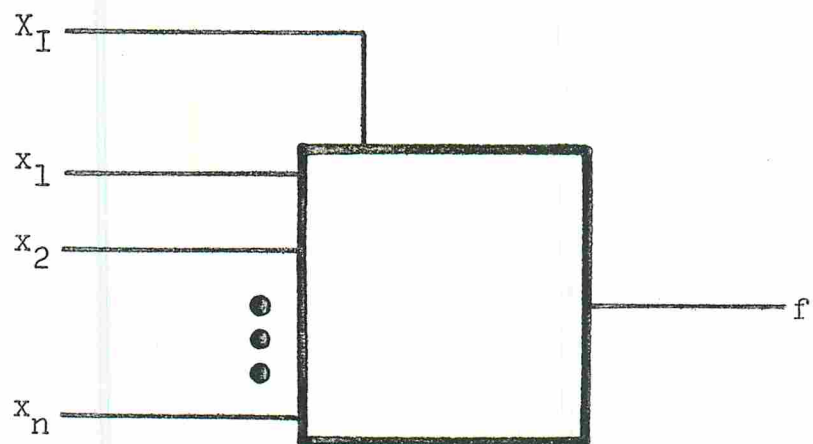


Figure 3.12. Intermittent fault model

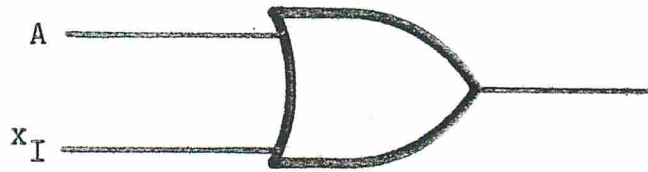


Figure 3.13. Model for intermittent fault  $f_{I1}$

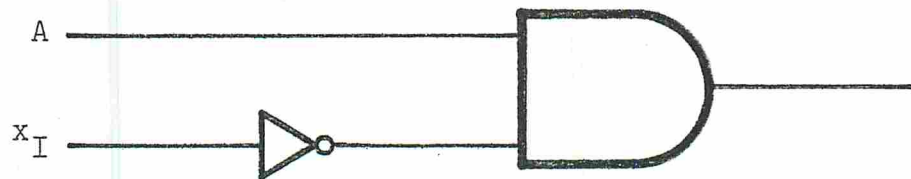


Figure 3.14. Model for intermittent fault  $f_{I0}$



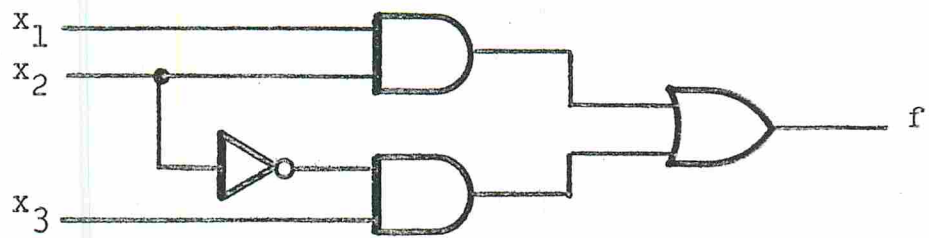


Figure 3.15. Circuit without the intermittent fault for Example 3.12

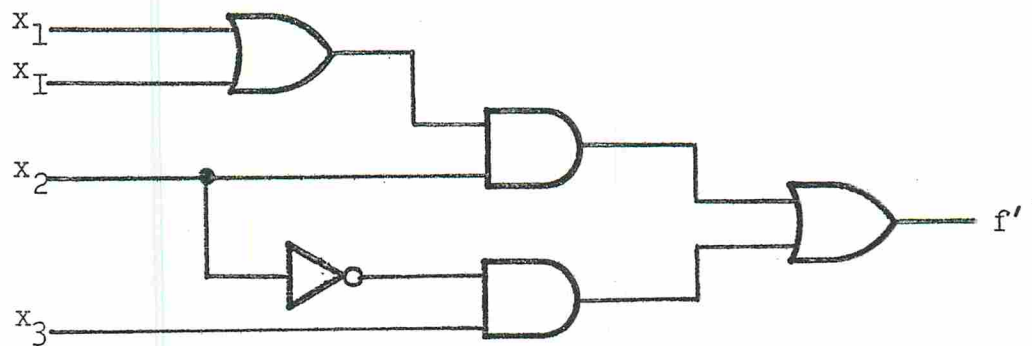


Figure 3.16. Modified circuit including the effect of intermittent fault  $f_{I1}$  for Example 3.12

$$F'(X_1, X_2, X_3, X_I) = X_2(X_1 + X_I - X_I X_I) + X_3(1 - X_2).$$

The intermittent fault is detected when  $f \oplus f' = 1$  and the probability of detecting the intermittent fault is given by  $F + F' - 2F \cdot F'$  (with exponents suppressed)

$$F + F' - 2F \cdot F' = X_I X_2 (1 - X_1) = X_I [X_2 (1 - X_1)].$$

But the probability of detecting the permanent fault  $x_1$  s-a-l equals  $X_2(1 - X_1)$ . Hence we can see that

probability of detecting  $f_{I1}$  = probability of detecting the corresponding permanent fault  $x_1$  s-a-l \* probability that the fault  $f_{I1}$  is present.

For the general case the following theorem applies.

Theorem 3.12: Let an intermittent fault and the corresponding permanent fault be denoted by  $f_I$  and  $f_i$ . Then

probability of detecting  $f_I$  = probability of detecting  $f_i$  \* probability  $f_I$  is present.

We will now derive expressions for the probability of detecting an intermittent fault in N patterns.

Case (i): Zero order Markov model

Here the probability that the intermittent fault is present is a constant  $p$ . Hence probability of not detecting an intermittent fault in  $N$  patterns =  $(1-a \cdot p)^N$  where  $a$  equals the probability of detecting the corresponding permanent fault. It follows that the probability of detecting an intermittent fault in  $N$  patterns equals

$$1 - (1-ap)^N.$$

Case (ii): First order discrete Markov model

Here the probability that the intermittent fault is present varies with discrete time. Let  $p_i$  be the probability that the fault is present at time  $t_i$ . Then the probability of detecting the intermittent fault equals

$$1 - [(1-ap_1)(a-ap_2) \cdots (1-ap_N)].$$

In this section we have introduced a model for introducing an intermittent fault into the circuit structure. Expressions for the probability of detecting an intermittent fault have been derived in terms of the probability of the intermittent fault's presence and the probabilities of input variables.

### 3.6 Concluding Remarks

In this chapter we have presented a procedure for algorithmic test generation for digital circuits. An algorithm for optimal random testing for permanent faults is also presented. Finally an intermittent fault model which takes into account circuit structure has been introduced. Using this, an optimal random testing strategy for a set of intermittent faults may be derived.

## CHAPTER 4

### PROBABILISTIC ASPECTS OF SYNCHRONOUS SEQUENTIAL CIRCUITS

#### 4.1 Introduction

In this chapter we will be dealing with the analysis of sequential circuits when input vectors are generated according to a given probability distribution. The theory developed in Chapters 2 and 3 will be extended to synchronous sequential circuits.

The problem of testing sequential circuits under random inputs has been dealt with previously [Br71, SM76, Lo77]. [Br71] deals with procedures for generating fault detection test sequences for sequential circuits. In this paper the author presents an adaptive random procedure, and discusses trade-offs between test generation time, test length, and percentage of faults detected. The concept of error latency [SM76] deals with the number of vectors applied between the occurrence of a fault and the first observation of an incorrect output. The error latency model provides one analysis of fault behavior in sequential circuits. This analysis can be used to specify a test length.

The analysis of compact testing of sequential circuits under random inputs has been discussed in [Lo77].



Compact testing is performed by comparing some statistic of the unit under test to the same statistic of the fault-free circuit.

A deterministic synchronizing sequence (DSS) is an input sequence which, when applied to a sequential circuit, results in a unique final state independent of the initial state.

A probabilistic synchronizing sequence (PSS) is a sequence of input patterns (generated according to a given input probability distribution) which when applied to a sequential circuit causes the feedback variables to converge to a steady state distribution independent of initial state distribution. We call this process probabilistic synchronization of the sequential circuit.

One of the major contributions in this chapter is the use of numerical analysis techniques for the analysis of sequential circuit behavior under random inputs.

In Section 4.2 we present a model for synchronous sequential circuits under random inputs. In Section 4.3 we develop the criteria for probabilistic synchronization of these circuits. In Section 4.4 we will present results on analyzing the probability distribution for the input vectors.

The theory developed can also be extended to intermittent fault testing in sequential circuits.



## 4.2 Model for Analysis of Synchronous Sequential Circuits under Random Inputs

In this section we will develop a model for a synchronous sequential circuit under random inputs.

A synchronous sequential circuit using only delay (D) flip-flops has the general form shown in Figure 4.1, where

$\underline{x} = (x_1, x_2, \dots, x_m)$  is the input vector,

$\underline{z} = (z_1, z_2, \dots, z_q)$  is the output vector,

$\underline{y} = (y_1, y_2, \dots, y_n)$  is the current state vector, and

$\underline{y}^+ = (y_1^+, y_2^+, \dots, y_n^+)$  is the next state vector.

On clocking,  $\underline{y}$  takes on the value of  $\underline{y}^+$ . In general we have

$$\underline{y}^+ = \underline{f}(\underline{y}, \underline{x})$$

$$\underline{z} = \underline{g}(\underline{y}, \underline{x}).$$

The row vector  $B$  was defined earlier in Chapter 2. We now present an equivalent definition.

Definition 4.1: Let  $\underline{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n)$ . Then  $B(\underline{\alpha})$  is given by the recursive relation

$$B(\alpha_1, \alpha_2, \dots, \alpha_n) \triangleq [B(\alpha_2, \alpha_3, \dots, \alpha_n) \mid \alpha_1 \cdot B(\alpha_2, \alpha_3, \dots, \alpha_n)]$$

where

$$B(\alpha_n) = [1 \mid \alpha_n].$$

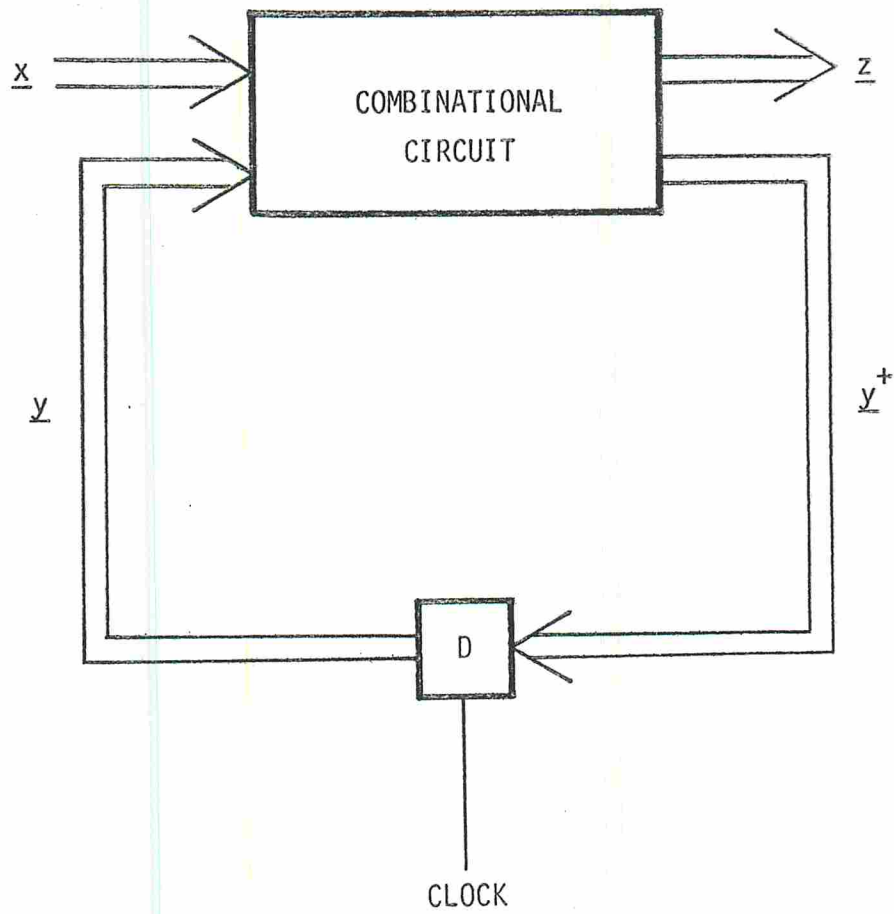


Figure 4.1. Synchronous sequential circuit using D flip-flops

Example 4.1: Let  $\underline{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$ .

$$B(\alpha_1, \alpha_2, \alpha_3) = [B(\alpha_2, \alpha_3) \mid \alpha_1 \cdot B(\alpha_2, \alpha_3)]$$

$$B(\alpha_2, \alpha_3) = [B(\alpha_3) \mid \alpha_2 \cdot B(\alpha_3)]$$

$$B(\alpha_3) = [1 \mid \alpha_3].$$

Hence  $B(\alpha_2, \alpha_3) = [1 \ \alpha_3 \ \alpha_2 \ \alpha_2 \alpha_3]$  and  $B(\alpha_1, \alpha_2, \alpha_3) = [1 \ \alpha_3 \ \alpha_2 \ \alpha_2 \alpha_3 \ \alpha_1 \ \alpha_1 \alpha_3 \ \alpha_1 \alpha_2 \ \alpha_1 \alpha_2 \alpha_3]$ .

It can be seen that  $B(\alpha_1, \alpha_2, \alpha_3)$  has 8 terms. It is obvious that, in general  $B(\alpha_1, \alpha_2, \dots, \alpha_n)$  has  $2^n$  terms.  $B(\underline{\alpha}; i)$  refers to the  $i^{th}$  component of  $B(\underline{\alpha})$ . If

$$\underline{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$$

then

$$B(\underline{\alpha}; 4) = \alpha_2 \alpha_3$$

and

$$B(\underline{\alpha}; 6) = \alpha_1 \alpha_3.$$

Definition 4.2: The matrix

$$A_f \triangleq \begin{bmatrix} A_{B(\underline{y}^+; 1)} \\ A_{B(\underline{y}^+; 2)} \\ \vdots \\ A_{B(\underline{y}^+; i)} \\ \vdots \\ A_{B(\underline{y}^+; 2^n)} \end{bmatrix}$$

where  $A_{B(\underline{y}^+;i)}$  is the minterm vector corresponding to the  $i^{th}$  component of  $B(\underline{y}^+)$  in terms of  $\underline{y}$  and  $\underline{x}$ . The  $j^{th}$  component of the vector  $A_{B(\underline{y}^+;i)} = 0(1)$  if and only if the minterm  $m_j$  is absent (present) in  $B(\underline{y}^+;i)$  where

$$m_j = \tilde{x}_1 \tilde{x}_2 \dots \tilde{x}_k \dots \tilde{x}_m \quad \tilde{y}_1 \tilde{y}_2 \dots \tilde{y}_\ell \dots \tilde{y}_n.$$

$\tilde{x}_k = x_k(\bar{x}_k)$  and  $\tilde{y}_\ell = y_\ell(\bar{y}_\ell)$  if and only if the corresponding component in the binary  $(m+n)$ -tuple representing integer  $j$  is 1(0).

Definition 4.3: The spectrum  $S_f$  of a synchronous sequential circuit is given by

$$S_f \stackrel{\Delta}{=} \begin{bmatrix} S_{B(\underline{y}^+;1)} \\ S_{B(\underline{y}^+;2)} \\ \vdots \\ S_{B(\underline{y}^+;i)} \\ \vdots \\ S_{B(\underline{y}^+;2^n)} \end{bmatrix}$$

where  $S_{B(\underline{y}^+;i)}$  is the spectrum of  $B(\underline{y}^+;i)$  over the variables  $\underline{x}$  and  $\underline{y}$ .

Theorem 4.1:  $S_f = A_f \cdot P$ .

Proof: Consider a component  $S_{B(\underline{y}^+;i)}$  of the spectrum  $S_f$ . It follows from Theorem 2.6 that  $S_{B(\underline{y}^+;i)} = A_{B(\underline{y}^+;i)}^P$  and the result follows. ■ ■

Let  $Y_i$  denote the probability that the variable  $y_i$  equals 1,  $i=1,2,\dots,n$ . Consider

$$Y = (Y_1, Y_2, \dots, Y_n) \quad \text{and} \quad \underline{X} = (X_1, X_2, \dots, X_m).$$

It is easy to show that

$$\begin{aligned} B(\underline{X}, \underline{Y}) = & [B(\underline{Y}) \mid X_m B(\underline{Y}) \mid X_{m-1} B(\underline{Y}) \mid X_{m-1} X_m B(\underline{Y}) \\ & \dots \mid X_1 B(\underline{Y}) \mid X_1 X_m B(\underline{Y}) \mid X_1 X_{m-1} B(\underline{Y}) \mid \\ & \dots \mid X_1 X_2 \dots X_m B(\underline{Y})]. \end{aligned}$$

It can be seen that  $B(\underline{X}, \underline{Y})$  has  $2^{(n+m)}$  terms.

Example 4.2: Let  $\underline{X} = (X)$  and  $\underline{Y} = (Y_1, Y_2)$

$$B(\underline{Y}) = [1 \ Y_2 \ Y_1 \ Y_1 Y_2]$$

and

$$B(\underline{X}, \underline{Y}) = [1 \ Y_2 \ Y_1 \ Y_1 Y_2 \ X \ XY_2 \ XY_1 \ XY_1 Y_2].$$

Theorem 4.2:  $B^T(\underline{Y}^+) = S_f B^T(\underline{X}, \underline{Y}) = A_f PB^T(\underline{X}, \underline{Y})$ .

Proof:  $PB^T(\underline{X}, \underline{Y})$  represents the probability of each min-term over  $\underline{y}$  and  $\underline{x}$  being 1. Consider the component  $B(\underline{y}^+; i)$ . Since  $A_{B(\underline{y}^+; i)}$  is the minterm vector corresponding to the  $i^{th}$  component of  $B(\underline{y}^+)$  we have  $B(\underline{y}^+; i) = A_{B(\underline{y}^+; i)} PB^T(\underline{X}, \underline{Y})$  and the result follows. ■ ■



Example 4.3: Consider the synchronous sequential machine given by the equation

$$y_1^+ = y_2(x \vee \bar{y}_1)$$

$$y_2^+ = \bar{y}_2 \vee x\bar{y}_1$$

where

$$B(\underline{y}^+) = (1 \ y_2^+ \ y_1^+ \ y_1^+y_2^+)$$

$$B(\underline{Y}^+) = (1 \ Y_2^+ \ Y_1^+ \ Y_1^+Y_2^+)$$

and

$$B(\underline{X}, \underline{Y}) = [1 \ Y_2 \ Y_1 \dots XY_1Y_2].$$

Table 4.1 shows the minterm vectors  $A_{B(\underline{y}^+; i)}$ ,  $i = 1, 2, 3, 4$ .

Then

$$A_f = \begin{bmatrix} A_{B(\underline{y}^+; 1)} \\ A_{B(\underline{y}^+; 2)} \\ A_{B(\underline{y}^+; 3)} \\ A_{B(\underline{y}^+; 4)} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Then

$$S_f = A_f \cdot P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}$$

and

Table 4.1. Minterm Vectors  $A_B(\underline{y}^+; i)$ ,  $i = 1, 2, 3, 4$

$x$	$y_1$	$y_2$	$A_B(\underline{y}^+; 1)$	$A_B(\underline{y}^+; 2)$	$A_B(\underline{y}^+; 3)$	$A_B(\underline{y}^+; 4)$
0	0	0	1	1	0	0
0	0	1	1	0	1	0
0	1	0	1	1	0	0
0	1	1	1	0	0	0
1	0	0	1	1	0	0
1	0	1	1	1	1	1
1	1	0	1	1	0	0
1	1	1	1	0	1	0

$$B^T(\underline{Y}^+) = A_f P B^T(\underline{X}, \underline{Y}) = \begin{bmatrix} 1 \\ 1 - Y_2 + XY_2 - XY_1 Y_2 \\ Y_2 - Y_1 Y_2 + XY_1 Y_2 \\ XY_2 - XY_1 Y_2 \end{bmatrix}.$$

An equivalent representation for  $B^T(\underline{Y}^+)$  which allows one to partition the  $\underline{X}$  and  $\underline{Y}$  variables is given in the following theorem.

Theorem 4.3:  $B^T(\underline{Y}^+) = D(\underline{X})B^T(\underline{Y})$ .

Proof: We know that  $B(\underline{Y}^+; i) = S_{B(\underline{Y}^+; i)} B^T(\underline{X}, \underline{Y})$ . Let  $e_{it}$  be the  $t^{th}$  component of  $S_{B(\underline{Y}^+; i)}$ . Hence

$$B(\underline{Y}^+; i) = \sum_{t=1}^{2^{(n+m)}} e_{it} (B(\underline{X}, \underline{Y}); t).$$

The components  $(B(\underline{X}, \underline{Y}); j), (B(\underline{X}, \underline{Y}); 2^n + j), \dots, (B(\underline{X}, \underline{Y}); 2^n(2^m - 1) + j)$  of  $B(\underline{X}, \underline{Y})$  are of the form  $\ell_j(\underline{X})B(\underline{Y}; j), \ell_{2^n+j}(\underline{X})B(\underline{Y}; j), \dots, \ell_{2^n(2^m-1)+j}(\underline{X})B(\underline{Y}; j)$  for  $j = 1, 2, \dots, 2^n$ . Let  $N_j = \{j, 2^n + j, 2 \cdot 2^n + j, 3 \cdot 2^n + j, \dots, (2^m - 1)2^n + j\}$  for  $j = 1, 2, \dots, 2^n$ . Hence

$$\begin{aligned} B(\underline{Y}^+; i) &= \sum_{t \in N_1} e_{it} (B(\underline{X}, \underline{Y}); t) + \sum_{t \in N_2} e_{it} (B(\underline{X}, \underline{Y}); t) \\ &+ \dots + \sum_{t \in N_{2^n}} e_{it} (B(\underline{X}, \underline{Y}); t). \end{aligned}$$

But

$$\begin{aligned} \sum_{t \in N_1} e_{it}(B(\underline{X}, \underline{Y}); t) &= B(\underline{Y}; 1) \sum_{t \in N_1} e_{it} l_t(\underline{X}) \\ &\vdots \\ \sum_{t \in N_{2^n}} e_{it}(B(\underline{X}, \underline{Y}); t) &= B(\underline{Y}; 2^n) \sum_{t \in N_{2^n}} e_{it} l_t(\underline{X}). \end{aligned}$$

Let

$$\begin{aligned} \sum_{t \in N_1} e_{it} l_t(\underline{X}) &= d_{i1}(\underline{X}) \\ &\vdots \\ \sum_{t \in N_{2^n}} e_{it} l_t(\underline{X}) &= d_{i2^n}(\underline{X}). \end{aligned}$$

Hence  $B(\underline{Y}^+; i) = \sum_{j=1}^{2^n} d_{ij}(\underline{X}) B(\underline{Y}; j)$  and the result follows. ■■

Example 4.4: Consider the sequential machine of Example 4.3.

$$B(\underline{Y}^+) = [1 \ Y_2^+ \ Y_1^+ \ Y_1^+ Y_2^+]$$

$$B(\underline{Y}) = [1 \ Y_2 \ Y_1 \ Y_1 Y_2]$$

and

$$B(\underline{X}, \underline{Y}) = [1 \ Y_2 \ Y_1 \ Y_1 Y_2 \ X \ XY_2 \ XY_1 \ XY_1 Y_2]$$

and

$$S_f = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}.$$

Consider the component  $B(\underline{Y}^+; 2)$  of  $B(\underline{Y}^+)$ .

$$\begin{aligned}
B(\underline{Y}^+;2) &= Y_2^+ = S_{B(\underline{Y}^+;2)} B^T(\underline{X}, \underline{Y}) \\
&= [1 \ -1 \ 0 \ 0 \ 0 \ 1 \ 0 \ -1] B^T(\underline{X}, \underline{Y})
\end{aligned}$$

components  $(B(\underline{X}, \underline{Y});1)$  and  $(B(\underline{X}, \underline{Y});5)$  are of the form  $1 \cdot B(\underline{Y};1)$  and  $X \cdot B(\underline{Y};1)$  respectively,

components  $(B(\underline{X}, \underline{Y});2)$  and  $(B(\underline{X}, \underline{Y});6)$  are of the form  $1 \cdot B(\underline{Y};2)$  and  $X \cdot B(\underline{Y};2)$  respectively,

components  $(B(\underline{X}, \underline{Y});3)$  and  $(B(\underline{X}, \underline{Y});7)$  are of the form  $1 \cdot B(\underline{Y};3)$  and  $X \cdot B(\underline{Y};3)$  respectively,

and

components  $(B(\underline{X}, \underline{Y});4)$  and  $(B(\underline{X}, \underline{Y});8)$  are of the form  $1 \cdot B(\underline{Y};4)$  and  $X \cdot B(\underline{Y};4)$  respectively.

$$N_1 = \{1, 5\}$$

$$N_2 = \{2, 6\}$$

$$N_3 = \{3, 7\}$$

$$N_4 = \{4, 8\}.$$

Hence

$$\begin{aligned}
B(\underline{Y}^+;2) &= \sum_{t \in \{1, 5\}} e_{it} (B(\underline{X}, \underline{Y});t) + \sum_{t \in \{2, 6\}} e_{it} (B(\underline{X}, \underline{Y});t) \\
&+ \sum_{t \in \{3, 7\}} e_{it} (B(\underline{X}, \underline{Y});t) + \sum_{t \in \{4, 8\}} e_{it} (B(\underline{X}, \underline{Y});t).
\end{aligned}$$

$$\begin{aligned}\sum_{t \in \{1,5\}} e_{it}(B(\underline{X}, \underline{Y}); t) &= B(\underline{Y}; 1) \sum_{t \in \{1,5\}} e_{it} \ell_t(\underline{X}) \\ &= B(\underline{Y}; 1)(1)\end{aligned}$$

$$\begin{aligned}\sum_{t \in \{2,6\}} e_{it}(B(\underline{X}, \underline{Y}); t) &= B(\underline{Y}; 2) \sum_{t \in \{2,6\}} e_{it} \ell_t(\underline{X}) \\ &= B(\underline{Y}; 2)(-1+X)\end{aligned}$$

$$\sum_{t \in \{3,7\}} e_{it}(B(\underline{X}, \underline{Y}); t) = B(\underline{Y}; 3) \sum_{t \in \{3,7\}} e_{it} \ell_t(\underline{X}) = 0$$

$$\begin{aligned}\sum_{t \in \{4,8\}} e_{it}(B(\underline{X}, \underline{Y}); t) &= B(\underline{Y}; 4) \sum_{t \in \{4,8\}} e_{it} \ell_t(\underline{X}) \\ &= B(\underline{Y}; 4)(-X) .\end{aligned}$$

Hence

$$\begin{aligned}B(\underline{Y}^+; 2) &= B(\underline{Y}; 1) \cdot 1 + B(\underline{Y}; 2)(-1+X) \\ &\quad + B(\underline{Y}; 3) \cdot 0 + B(\underline{Y}; 4)(-X) .\end{aligned}$$

Similarly we can show that

$$B(\underline{Y}^+; 1) = B(\underline{Y}; 1) \cdot 1$$

$$B(\underline{Y}^+; 3) = B(\underline{Y}; 2) \cdot 1 + B(\underline{Y}; 4)(-1+X)$$

and

$$B(\underline{Y}^+; 4) = B(\underline{Y}; 2) \cdot X + B(\underline{Y}; 6)(-X) .$$

Hence



$$B^T(\underline{Y}^+) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & (-1+X) & 0 & -X \\ 0 & 1 & 0 & (-1+X) \\ 0 & X & 0 & -X \end{bmatrix} \begin{bmatrix} B(\underline{Y};1) \\ B(\underline{Y};2) \\ B(\underline{Y};3) \\ B(\underline{Y};4) \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & (-1+X) & 0 & -X \\ 0 & 1 & 0 & (-1+X) \\ 0 & X & 0 & -X \end{bmatrix} \begin{bmatrix} 1 \\ Y_2 \\ Y_1 \\ Y_1 Y_2 \end{bmatrix}$$

In the appendix we show how the Reed-Muller form for  $y_i^+ = f(\underline{y}, \underline{x})$  can be easily obtained from  $B^T(\underline{Y}^+) = D(\underline{X})B^T(\underline{Y})$ .

It can be seen that the first row of the matrix  $D(\underline{X})$  is  $[1 \ 0 \ 0 \ \dots \ 0]$ . During the course of further discussions, the components  $B(\underline{Y}^+;1)$  and  $B(\underline{Y};1)$  will not be used. The vector  $B(\underline{\alpha})$  without the component  $B(\underline{\alpha};1)$  will be denoted by  $L(\underline{\alpha})$ .

We then have

$$\begin{bmatrix} 1 \\ \hline L(\underline{Y}^+)^T \end{bmatrix} = \begin{bmatrix} 1 & | & 0 \dots 0 \\ \hline d_{21} & & \\ \vdots & & \\ d_{2n1} & & \end{bmatrix} \begin{bmatrix} 1 \\ \hline L(\underline{Y})^T \end{bmatrix}$$

$C(\underline{X})$

and

$$L(\underline{Y}^+) = C(\underline{X})L(\underline{Y})^T + E$$

where

$$E = \begin{bmatrix} d_{21} \\ \vdots \\ d_{2n_1} \end{bmatrix}.$$

Using this new notation, the sequential circuit of Example 4.4 can be represented as

$$\begin{bmatrix} Y_2^+ \\ Y_1^+ \\ Y_1^+ Y_2^+ \end{bmatrix} = \begin{bmatrix} (-1+X) & 0 & -X \\ 1 & 0 & (-1+X) \\ X & 0 & -X \end{bmatrix} \begin{bmatrix} Y_2 \\ Y_1 \\ Y_1 Y_2 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

### 4.3 Probabilistic Synchronization

In this section we discuss the criteria for probabilistic synchronization of sequential circuits.

A deterministic synchronizing sequence (DSS) is an input sequence which, when applied to a sequential circuit, results in a unique final state independent of the initial state. This may be viewed as the convergence of the machine to a final state independent of the initial state.

It is possible to generate a deterministic synchronizing sequence by constructing a synchronizing tree. This method is illustrated on the state table shown in Figure 4.2. The synchronizing tree is constructed in Figure 4.3. Each node of the tree is a set of states and the branches indicate applying values to the input  $x$  leading to a new

Previous State	Next State	
	x = 0	x = 1
1	1	3
2	2	3
3	2	4
4	1	2

Figure 4.2. State table for a sequential circuit

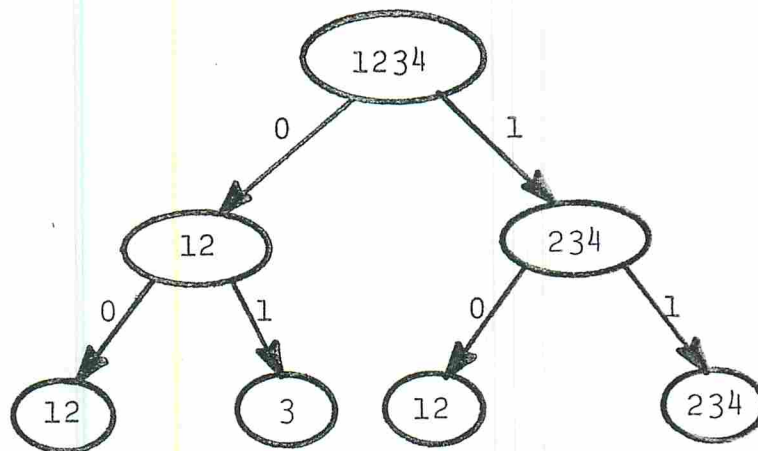


Figure 4.3. Synchronizing tree for the sequential circuit of Fig.4.2

set of states. The tree is pruned when a previously generated node is generated again. A synchronizing sequence is represented by a path leading from the root to a node consisting of one state only. Not all sequential machines have synchronizing sequences.

We have, in the previous section, established a model for a synchronous circuit of the form  $L(\underline{Y}^+)^T = C(\underline{X})L(\underline{Y})^T + E$  where  $C(\underline{X})$  is a matrix. Consider a JK flip-flop with inputs  $j$  and  $k$ , whose characteristic equation is given by

$$y^+ = j\bar{y} \vee \bar{k}y.$$

The corresponding probability expression model is given by  $Y^+ = J(1-Y) + (1-K)Y = J + Y(1-J-K)$  where  $J = \Pr(j = 1)$  and  $K = \Pr(k = 1)$ .

Let  $Y(t)$  denote the  $\Pr(y = 1)$  at time  $t$ .

Case 1: Let  $J = 0.2$  and  $K = 0.6$ .

We have

$$\begin{aligned} Y(1) &= 0.2 + 0.2(Y(0)) \\ Y(2) &= 0.2 + 0.2Y(1) \\ &= 0.2 + (0.2)^2 + (0.2)^2 Y(0) \\ Y(3) &= 0.2 + (0.2)^2 + (0.2)^3 + (0.2)^2 Y(0) \\ &\vdots \end{aligned}$$

We see that the contribution of  $Y(0)$  to  $Y(t)$  diminishes as  $t$  increases and for large  $t$ ,  $Y(t)$  approaches the limiting

value of 0.25 independent of  $Y(0)$ .

Case 2: Let us consider the case  $J = 1, K = 0$

$$Y(1) = 1 + Y(0) \cdot 0 = 1$$

$$Y(2) = 1 + Y(1) \cdot 0 = 1$$

and hence  $Y(t)$  converges very rapidly to its limiting value  $Y(t) = 1$ .

Case 3: Let us consider the case  $J = 1, K = 1$

$$Y(1) = 1 + Y(0)[1 - 1 - 1]$$

$$= 1 - Y(0)$$

$$Y(2) = 1 - Y(1) = 1 - [1 - Y(0)] = Y(0)$$

$$Y(3) = 1 - Y(2) = 1 - Y(0)$$

$$\vdots$$

We see that  $Y(t)$  does not converge and oscillates between the two values  $Y(0)$  and  $1 - Y(0)$ .

We recall at this stage that  $J = 1, K = 0$  corresponds to the synchronizing input sequence ( $j = 1, k = 0$ ) and that  $J = 1, K = 1$  corresponds to the toggling condition  $j = 1, k = 1$ . Thus in the case  $J = 1, K = 1$  we see that the effect of  $Y(0)$  persists for all time  $t$ .

One of the drawbacks associated with random testing of synchronous circuits is the "ineffectiveness" of random inputs to effectively initialize the circuit. We say that the steady state probability distribution corresponds to



initializing the circuit under random inputs.

In this section we establish the criteria under which the feedback variables of a synchronous sequential circuit converge to a steady state distribution independent of the initial state distribution.

Definition 4.4: The steady state probability distribution  $L_s(\underline{Y}^+)$  of a synchronous circuit corresponds to the condition  $\underline{Y}^+ = \underline{Y}$ .

Definition 4.5: The Infinity Norm of a matrix  $C$  is defined by  $\|C\| = \max_i (\sum_j |C_{ij}|)$ .

Let  $\underline{A}$  be a vector of real numbers in the interval  $[0,1]$  assigned to  $\underline{X}$ .

Definition 4.6: The spectral radius  $S(C, \underline{A})$  of the matrix  $C$  under assignment  $\underline{X} = \underline{A}$  is defined by  $S(C, \underline{A}) = \max \{ |\lambda| : \lambda \in \sigma(C, \underline{A}) \}$  where  $\sigma(C, \underline{A})$  is the set of all eigenvalues of  $C$  under assignment  $\underline{X} = \underline{A}$ .

Theorem 4.4: Let  $\underline{Y}(0), \underline{Y}(1), \underline{Y}(2), \dots, \underline{Y}(N)$  be the state probability distribution of a synchronous sequential circuit at time  $t = 0, 1, 2, \dots, N$ . The series  $(\underline{Y}(0), \underline{Y}(1), \dots, \underline{Y}(N), \dots)$  converges for  $\underline{X} = \underline{A}$  if and only if the spectral radius  $S(C, \underline{A}) < 1$ .



Proof: We know that  $L(\underline{Y}^+)^T = C(\underline{X})L(\underline{Y})^T + E$ . Under the assignment  $\underline{X} = \underline{A}$  we have

$$\begin{aligned} L(\underline{Y}(1))^T &= C(\underline{A})L(\underline{Y}(0))^T + E \\ L(\underline{Y}(2))^T &= C(\underline{A})L(\underline{Y}(1))^T + E \\ &= C^2(\underline{A})L(\underline{Y}(0))^T + C(\underline{A})E + E \\ &\vdots \\ L(\underline{Y}(N+1))^T &= C^{N+1}(\underline{A})L(\underline{Y}(0))^T + E(I + C(\underline{A}) + C^2(\underline{A}) + \dots + C^N(\underline{A})). \end{aligned}$$

The series  $(I + C(\underline{A}) + C^2(\underline{A}) + \dots + C^N(\underline{A}) + \dots)$  converges if and only if [B165]

- (1)  $S(C, \underline{A}) < 1$  or
- (2)  $\lim_{p \rightarrow \infty} C^p(\underline{A}) = 0$  or
- (3)  $\lim_{p \rightarrow \infty} \|C^p(\underline{A})\|^{1/p} < 1$

Case 1: Assume  $S(C, \underline{A}) < 1$ .

$$\text{Hence } \lim_{N \rightarrow \infty} (C^N(\underline{A})) = 0.$$

The term  $C^{N+1}(\underline{A})L(\underline{Y}(0))^T \rightarrow 0$  as  $N \rightarrow \infty$  and the series  $(I + C(\underline{A}) + C^2(\underline{A}) + \dots + C^N(\underline{A}) + \dots)$  converges.

Therefore  $L(\underline{Y}(N+1))^T$  converges.

Case 2: Assume  $S(C, \underline{A}) \nless 1$ .

Then the series  $(I + C(\underline{A}) + C^2(\underline{A}) + \dots + C^N(\underline{A}) + \dots)$  does not converge and hence  $L(\underline{Y}(N+1))^T$  does not converge. ■ ■

A simpler, but sufficient, condition for the series

$(\underline{Y}(0), \underline{Y}(1), \dots, \underline{Y}(N), \dots)$  to converge is given by  $\|C(\underline{A})\| < 1$ .

In the following theorem we will establish that there exists an assignment  $\underline{X} = \underline{A}$  for any strongly connected synchronous circuits such that  $S(C, \underline{A}) < 1$ . The implication is that there always exists an  $\underline{A}$  so that a steady state probability distribution is achieved for such a synchronous circuit.

Theorem 4.5: There exists an assignment  $\underline{X} = \underline{A}$  for a strongly connected synchronous circuit such that  $S(C, \underline{A}) < 1$ .

Proof: Let  $m(\underline{y})$  be the vector consisting of all the min-terms over  $\underline{y}$ . The components of  $m(\underline{y})$  are ordered by the corresponding decimal numbers. Let  $M(\underline{Y})$  be the vector of probability expressions of  $m(\underline{y})$ .

From Theorem 2.6 we have

$$M(\underline{Y})^T = P \cdot B(\underline{Y})^T$$

and from Theorem 4.2, we have

$$B(\underline{Y}^+)^T = D(\underline{X})B(\underline{Y})^T.$$

Therefore

$$P^{-1}M(\underline{Y}^+)^T = D(\underline{X})P^{-1}M(\underline{Y})^T$$

and

$$M(\underline{Y}^+)^T = (PD(\underline{X})P^{-1})M(\underline{Y})^T$$

is an equivalent representation for the sequential circuit.

The matrix  $G(\underline{X}) \triangleq PD(\underline{X})P^{-1}$  is essentially a state transition probability matrix. Each entry of the matrix  $G(\underline{X})$  takes values from the interval  $[0,1]$  and each column has the property that the sum of all elements in that column equals one. Hence  $G(\underline{X})$  is a stochastic matrix [KS60], and corresponds to a finite first order monodesmic Markov chain. It has been shown that, for such a matrix, there exists an assignment  $\underline{X} = \underline{A}$  so that there is exactly one eigenvalue of value one and all other eigenvalues having absolute values less than one. Since all the eigenvalues of  $P$  and  $P^{-1}$  are equal to one, and  $G(\underline{X})$  and  $D(\underline{X})$  are similar (and equivalent)  $G(\underline{X})$  and  $D(\underline{X})$  have the same eigenvalues. But

$$D(\underline{X}) = \left[ \begin{array}{c|cccc} 1 & 0 & 0 & \dots & 0 \\ \hline E & & C(\underline{X}) & & \end{array} \right].$$

Therefore  $D(\underline{X})$  has all the eigenvalues of  $C(\underline{X})$  in addition to the eigenvalue  $\lambda = 1$ .

Hence,  $S(C, \underline{A}) < 1$ .

Theorem 4.6: The steady state probability distribution  $L_s(\underline{Y}^+)$  of a sequential circuit is given by  $L_s(\underline{Y}^+)^T = [I - C(\underline{A})]^{-1}E$ , if it exists.

Proof: If  $L_s(\underline{Y}^+)$  exists we have

$$L_s(\underline{Y}^+)^T = C(\underline{A})L_s(\underline{Y}^+)^T + E.$$

Hence

$$[I - C(\underline{A})]L_s(\underline{Y}^+) = E$$

and

$$L_s(\underline{Y}^+)^T = [I - C(\underline{A})]^{-1}E.$$

Example 4.5: Consider the sequential machine given by the equations

$$y_1^+ = xy_2$$

$$y_2^+ = x\bar{y}_1.$$

Hence

$$\begin{bmatrix} y_2^+ \\ y_1^+ \\ y_1^+ y_2^+ \end{bmatrix} = \begin{bmatrix} 0 & -x & 0 \\ x & 0 & 0 \\ x & 0 & -x \end{bmatrix} \begin{bmatrix} y_2 \\ y_1 \\ y_1 y_2 \end{bmatrix} + \begin{bmatrix} x \\ 0 \\ 0 \end{bmatrix}.$$

The eigenvalues  $\sigma(C, \underline{A})$  are given by solving the equation  $\text{Det}(\lambda I - C(\underline{A})) = 0$ .

$$\lambda I - C(\underline{A}) = \begin{bmatrix} \lambda & A & 0 \\ -A & \lambda & 0 \\ -A & 0 & \lambda + A \end{bmatrix}$$

$$\begin{aligned} \text{Det}(\lambda I - C) &= \lambda^2(\lambda + A) - A(-A)(\lambda + A) \\ &= (\lambda + A)(\lambda^2 + A^2). \end{aligned}$$

Hence

$$\sigma(C, \underline{A}) = \{-A, \pm iA\}.$$

The spectral radius  $S(C, \underline{A}) = A$  and the machine converges if and only if  $A < 1$ . The corresponding

$$\begin{aligned} L_S(\underline{Y}^+) &= [I - C(\underline{A})]^{-1} E \\ &= \begin{bmatrix} A(1+A)/A^3 + A^2 + A + 1 \\ A^2(1+A)/A^3 + A^2 + A + 1 \\ A^2/A^3 + A^2 + A + 1 \end{bmatrix}. \end{aligned}$$

We now consider the following cases.

Case 1:  $A = 0$ .

We know the machine converges and

$$\begin{aligned} L_S(\underline{Y}^+) &= \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \\ L(\underline{Y}(1)) &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} Y_2(0) \\ Y_1(0) \\ Y_1(0)Y_2(0) \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \end{aligned}$$

and the number of vectors required for achieving a steady

state probability distribution equals 1. It is interesting to note that we have generated a DSS in this case.

Case 2:  $A = 1$ .

We know that the machine does not converge and we will show that the effect of  $\underline{Y}(0)$  persists for any time  $t$ .

$$L(\underline{Y}(1)) = C(\underline{A})L(\underline{Y}(0)) + E$$

$$= \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & -1 \end{bmatrix} L(\underline{Y}(0)) + E$$

$$L(\underline{Y}(2)) = C(\underline{A})L(\underline{Y}(1)) + E$$

$$= C^2(\underline{A})L(\underline{Y}(0)) + C(\underline{A})E + E$$

$$= \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ -1 & -1 & 1 \end{bmatrix} L(\underline{Y}(0)) + E(I + C(\underline{A}))$$

$$L(\underline{Y}(3)) = C^3(\underline{A})L(\underline{Y}(0)) + E(I + C(\underline{A}) + C^2(\underline{A}))$$

$$= \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 1 & -1 \end{bmatrix} L(\underline{Y}(0)) + E(I + C(\underline{A}) + C^2(\underline{A}))$$

$$L(\underline{Y}(4)) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} L(\underline{Y}(0)) + E(I + C(\underline{A}) + C^2(\underline{A}) + C^3(\underline{A})).$$

Since



$$I + C(\underline{A}) + C^2(\underline{A}) + C^3(\underline{A}) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

we have

$$L(\underline{Y}(4)) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} L(\underline{Y}(0))$$

$$L(\underline{Y}(5)) = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & -1 \end{bmatrix} L(\underline{Y}(0)) \\ + E(I + C(\underline{A}) + C^2(\underline{A}) + C^3(\underline{A}) + C^4(\underline{A})).$$

Since

$$I + C(\underline{A}) + C^2(\underline{A}) + C^3(\underline{A}) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

and

$$C^4(\underline{A}) = I$$

we have

$$L(\underline{Y}(5)) = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & -1 \end{bmatrix} L(\underline{Y}(0)) + E \\ = L(\underline{Y}(1)).$$

It can be shown that for  $i = 1, 2, 3, 4$

$$L(\underline{Y}(4k+i)) = L(\underline{Y}(i)) \quad k = 1, 2, 3, \dots$$

Hence the effect of  $L(\underline{Y}(0))$  persists for any time  $t$ .

Definition 4.7: Let  $e(m) = L(\underline{Y}(m)) - L_S(\underline{Y})$ . The rate of convergence  $R$  of a synchronous sequential circuit is given by  $R = \frac{1}{N}$ , where  $N$  is the smallest integer such that

$$\frac{\|e(N)\|}{\|e(0)\|} \leq \frac{1}{e}$$

and  $e$  is the base of the natural system of logarithms.

Theorem 4.7: The rate of convergence  $R$  is directly proportional to  $\log\left(\frac{1}{S(C, \underline{A})}\right)$ .

Proof:  $e(m+1) = L(\underline{Y}(m+1)) - L_S(\underline{Y})$ .

Since

$$L(\underline{Y}(m+1)) = C(\underline{A})[L(\underline{Y}(m))] + E$$

and

$$L_S(\underline{Y}) = C(\underline{A})L_S(\underline{Y}) + E$$

$$e(m+1) = C(\underline{A})[L(\underline{Y}(m)) - L_S(\underline{Y})]$$

$$e(m+1) = C(\underline{A})e(m)$$

$$= C^2(\underline{A})e(m-1)$$

$$\vdots$$

$$e(m+1) = C^{m+1}(\underline{A})e(0).$$

Hence

$$\frac{e(m+1)}{e(0)} = C^{m+1}(\underline{A}).$$

The ratio

$$\begin{aligned}\frac{\|e(m+1)\|}{\|e(0)\|} &\cong \|C^{m+1}(\underline{A})\| \\ \|C^{m+1}(\underline{A})\| &= \|C^{\frac{m+1}{p} \cdot p}(\underline{A})\| \\ &\cong (\|C^p(\underline{A})\|^{1/p})^{m+1} \\ &= [S(C, \underline{A})]^{m+1}.\end{aligned}$$

Hence

$$\frac{\|e(m+1)\|}{\|e(0)\|} \cong [S(C, \underline{A})]^{m+1}.$$

Let  $N$  be the smallest integer such that

$$\frac{\|e(N)\|}{\|e(0)\|} \cong \frac{1}{\epsilon}.$$

It suffices if  $[S(C, \underline{A})]^N \cong \frac{1}{\epsilon}$ .

Hence

$$N = \frac{\log \epsilon}{\log \left( \frac{1}{S(C, \underline{A})} \right)}$$

and

$$R = \log \left( \frac{1}{S(C, \underline{A})} \right) / \log \epsilon. \quad \blacksquare \blacksquare$$

It can be seen that if  $S(C, \underline{A})$  is close to one, the convergence is slow. Convergence is faster when  $S(C, \underline{A})$  is closer to zero.

Example 4.6: Consider the sequential circuit given by the following state table, and which has the synchronizing sequence 01.

PS	NS	
	x = 0	x = 1
1	1	3
2	2	3
3	2	4
4	1	2

The feedback equations are given by

$$y_1^+ = xy_2 \vee x\bar{y}_1$$

$$y_2^+ = \bar{x}y_2 \vee x\bar{y}_1 \vee x\bar{y}_2.$$

Hence we have

$$\begin{bmatrix} y_2^+ \\ y_1^+ \\ y_1^+ y_2^+ \end{bmatrix} = \begin{bmatrix} (1-X) & 0 & -X \\ 0 & -X & X \\ 0 & -X & 0 \end{bmatrix} \begin{bmatrix} y_2 \\ y_1 \\ y_1 y_2 \end{bmatrix} + \begin{bmatrix} X \\ X \\ X \end{bmatrix}.$$

The eigenvalues of the matrix  $C(A)$  are given by

$$\lambda_1 = 1-A, \quad \lambda_2 = \frac{-A+j\sqrt{3A}}{2}$$

and

$$\lambda_3 = \frac{-A-j\sqrt{3A}}{2}.$$

The magnitude of the eigenvalues  $\lambda_2$  and  $\lambda_3$  equals

$$\sqrt{\frac{A^2 + 3A^2}{4}} = A.$$

Hence the spectral radius  $S(C,A) = \max(1-A, A)$ . Figure 4.4 shows the spectral radius  $S(C,A)$  as  $A$  varies. We see that  $S(C,A) = 1$  when  $A = 1$  or  $A = 0$ . It can be seen that when  $A = 1$  or  $A = 0$  the effect of the initial state  $Y(0)$  persists for any time  $t$ .

If  $L_S(\underline{Y}^+)$  exists, then

$$L_S(\underline{Y}^+) = \begin{bmatrix} 1-A^2/1+A+A^2 \\ A(1+A)/1+A+A^2 \\ A/1+A+A^2 \end{bmatrix}.$$

We know that the minimum value of  $S(C,A) = 0.5$  and

$$L_S(\underline{Y}^+) = \begin{bmatrix} 0.75/1.75 \\ 0.75/1.75 \\ 0.5/1.75 \end{bmatrix} = \begin{bmatrix} 3/7 \\ 3/7 \\ 2/7 \end{bmatrix}.$$

The rate of convergence  $R = \frac{1}{N}$  where

$$N = \frac{\log \epsilon}{\log 2} = \frac{0.4343}{0.3010} = 1.43.$$

Hence

$$R = \frac{1}{1.43} = 0.65.$$

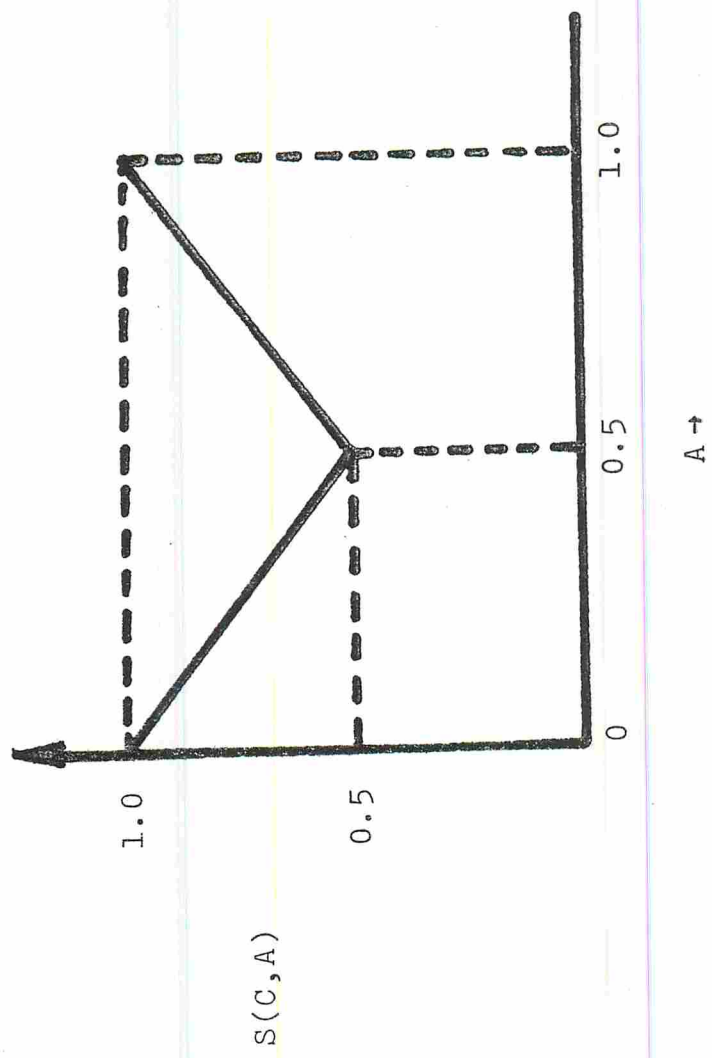


Figure 4.4. Relationship between  $A$  and  $S(C,A)$  for the circuit of Example 4.6.



We also compute the number of vectors,  $N$ , needed for the condition

$$\frac{\|e^N\|}{\|e^0\|} \cong 0.0001.$$

Here

$$N = \frac{\log(10^{-4})}{\log[S(C,A)]} = \frac{4}{\log 2} = \frac{4}{0.3010} = 14.$$

Therefore 14 vectors are needed to achieve  $L_s(\underline{Y}^+)$  to an accuracy of 0.0001.

In this section, we have defined the steady state probability distribution  $L_s(\underline{Y}^+)$  of a synchronous sequential circuit. We have established the criterion for convergence to  $L_s(\underline{Y}^+)$  of these circuits. A procedure to evaluate  $L_s(\underline{Y}^+)$  was presented. The relationship between the input probability distribution and the rate of convergence to  $L_s(\underline{Y}^+)$  was also discussed.

#### 4.4 Analysis of Synchronous Sequential Circuits under Faulty Conditions

In this section we will analyze the behavior of synchronous circuits under faulty conditions. A model for the normal (fault-free) and faulty circuits, when input patterns are generated according to a given probability distribution, is presented. The probability of detecting a fault can be derived from this model.

We will assume that the machine corresponding to the circuit under consideration is strongly connected. We will also assume that the faulty circuit is strongly connected.

#### 4.4.1 Fault Model

The fault model used in this section is the stuck line fault model. Consider a specific fault  $b$ . Let

$$\underline{y}_b = (y_{b_1}, y_{b_2}, \dots, y_{b_n})$$

$$\underline{y}_b^+ = (y_{b_1}^+, y_{b_2}, \dots, y_{b_n})$$

and

$$\underline{z}_b = (z_{b_1}, z_{b_2}, \dots, z_{b_q})$$

denote the current state vector, the next state vector and the output vector of the sequential circuit under the fault  $b$ . The equations of the normal circuit and faulty circuit are given by

$$\underline{y}^+ = \underline{f}(\underline{y}, \underline{x})$$

$$\underline{z} = \underline{g}(\underline{y}, \underline{x})$$

and

$$\underline{y}_b^+ = \underline{f}_b(\underline{y}_b, \underline{x})$$

and

$$\underline{z}_b = \underline{g}_b(\underline{y}_b, \underline{x})$$

respectively.

A vector used to indicate the detection of a fault is defined by the equation

$$\underline{z}_{\text{det}} = \underline{z} \oplus \underline{z}_b.$$

Let  $\underline{y}_b = \Pr(\underline{y}_b = 1)$  and  $\underline{z}_b = \Pr(\underline{z}_b = 1)$ . Then

$$L(\underline{y}_b^+)^T = C_b(\underline{X}) \cdot L(\underline{y}_b)^T + E_b$$

and

$$\underline{z}_b = C'_b(\underline{X}) L(\underline{y}_b)^T + E'_b.$$

#### 4.4.2 Procedure to Determine the Probability of Detecting a Fault

We will now present a numerical procedure for determining the probability of detecting a fault in  $p$  patterns where  $p$  is the number of input patterns to be applied. The input probability distribution  $\underline{X} = \underline{A}$  is given.

Assume that the steady state probability distribution of a circuit has been reached. Let  $\underline{Y}(t)$  represent the probability distribution of  $\underline{y}$  after the application of the  $t^{\text{th}}$  pattern. For the sake of simplicity, we assume that the circuit has one output. Let  $\underline{z}_{\text{det}} = \Pr(\underline{z}_{\text{det}} = 1)$  where  $\underline{z}_{\text{det}} = \underline{z} \oplus \underline{z}_b$ .

Procedure 4.1: Procedure to evaluate the probability of detecting a fault in  $p$  patterns, given

$$\underline{X} = \underline{A}.$$

Let  $L_s(\underline{Y})$  and  $L_s(\underline{Y}_b)$  be the steady state probability distribution of the normal and faulty circuits

1. set  $L(\underline{Y}(0)) = L_s(\underline{Y})$ .
2. set  $L(\underline{Y}_b(0)) = L_s(\underline{Y}_b)$ .

3. compute

$$L(\underline{Y}(t))^T = C(\underline{A})L(\underline{Y}(t-1))^T + E$$

and

$$L(\underline{Y}_b(t))^T = C_b(\underline{A})L(\underline{Y}_b(t-1))^T + E_b$$

for  $t = 1, 2, \dots, p$ .

4. compute  $Z_{\text{det}}(t)$ ,  $t = 1, 2, \dots, p$ .

5. the probability of detecting fault  $b$  at pattern  $t = p$  is given by

$$1 - \prod_{t=0}^p (1 - Z_{\text{det}}(t)).$$

Example 4.7: Consider the circuit represented by

$$y_1^+ = \bar{x}y_1 \vee \bar{y}_1\bar{y}_2$$

$$y_2^+ = y_1$$

and

$$z = y_1.$$

Let the fault under consideration be  $y_1$  s-a-l. The faulty circuit is therefore represented by

$$y_{b1}^+ = \bar{x}$$

$$y_{b2}^+ = 1$$

and

$$z_b = 1.$$

Hence  $z_{\text{det}} = 1 \oplus y_1 = \bar{y}_1$ .

The equations of the normal and faulty circuit are given by

$$\begin{bmatrix} Y_2^+ \\ Y_1^+ \\ Y_1^+ Y_2^+ \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ -1 & -X & 1 \\ 0 & (1-X) & 0 \end{bmatrix} \begin{bmatrix} Y_2 \\ Y_1 \\ Y_1 Y_2 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

and

$$\begin{bmatrix} Y_{b2}^+ \\ Y_{b1}^+ \\ Y_{b1}^+ Y_{b2}^+ \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} Y_{b2} \\ Y_{b1} \\ Y_{b1} Y_{b2} \end{bmatrix} + \begin{bmatrix} 1 \\ 1-X \\ 1-X \end{bmatrix}.$$

Both the normal and the faulty circuit can be synchronized using  $\underline{X} = \underline{0}$  and

$$L_s(\underline{Y}^+) = L_s(\underline{Y}_b^+) = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

Let us compute the probability of detecting  $y_1$  s-a-l by applying vectors at the probability distribution  $X = 0.5$  after both the machines have been synchronized.

$$L(\underline{Y}(t))^T = \begin{bmatrix} 0 & 1 & 0 \\ -1 & -X & 1 \\ 0 & (1-X) & 0 \end{bmatrix} L(\underline{Y}(t-1))^T + \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

where

$$L(\underline{Y}(0)) = L_s(\underline{Y}^+) = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

It can be seen that

$$Y_1(0) = 1$$

$$Y_1(1) = 0.5$$

$$Y_1(2) = 0.25$$

$$Y_1(3) = 0.625$$

$$Y_1(4) = 0.5625.$$

Since  $Z_{\text{det}} = 1 - Y_1$ , the probability of detecting fault b at pattern  $t = 4$  is given by

$$1 - \prod_{t=0}^4 Y_1(t) = 1 - (0.5 \times 0.25 \times 0.625 \times 0.5625) = 0.96.$$

#### 4.5 Conclusions

In this chapter we have introduced a model for the analysis of synchronous sequential circuits under random inputs. Using classical numerical analysis techniques, we have established the criterion for probabilistic synchronization of these circuits. The relationship between the input probability distribution and the rate of convergence is discussed. Finally, a model for the analysis of syn-



chronous circuits under normal (fault-free) and faulty conditions is presented. This model is used to determine the probability of detecting a fault. This theory can be easily extended to the problem of intermittent fault testing in synchronous circuits by employing the model developed in Chapter 3.

## CHAPTER 5

### MULTIPLE OPERATING POINT RANDOM TESTING OF COMBINATIONAL CIRCUITS

#### 5.1 Introduction

The problem of determining the effectiveness of applying random input patterns in testing digital circuits has been studied previously. In this chapter we shall consider techniques to improve the "effectiveness" of random testing by applying random patterns using more than one input probability distribution, each one of which represents an operating point. This concept can be viewed as an application of deterministic testing concepts in random testing. In deterministic testing we apply a complete test set  $T_D$  (which detects all faults under consideration) to the circuit. One can view this as testing the circuit at  $m$  operating points by applying one pattern at each operating point.  $m$  is the cardinality of  $T_D$ . The concept of multiple operating point random testing deals with the application of random patterns at each operating point (which represents one input probability distribution).

Considerable work has already been done dealing with analytical measures used in *single* operating point random

testing. One analytic measure [AA75a,AA76] is based on the probability of sensitizing the longest path in a NAND tree network. Based on this circuit topology, the optimal input probability distribution can be determined. Another measure is the expected number of faults detected as a function of the number of input patterns applied [HB73]. The error latency of a fault [SM75,SM76] and maximizing the probability of the "hardest" fault to detect under equiprobable inputs [DB76] have also been studied as other analytical measures.

## 5.2 Functions Used in Multiple Operating Point Random Testing

In this section we will define the functions to be used in the generation of multiple operating point random tests for combinational circuits. The relationship between these functions is also derived.

Definition 5.1: An operating point  $OP_j$  is defined by  $OP_j \triangleq (X_{1j}, X_{2j}, \dots, X_{nj})$  where  $X_{ij} = \Pr(x_i=1)$ ,  $i = 1, 2, \dots, n$ .  $T_j$  represents the set of patterns applied at  $OP_j$ .

Definition 5.2: A multiple operating point is defined by  $OP^{(\ell)} \triangleq (OP_1, OP_2, \dots, OP_\ell)$ .  $T^\ell \triangleq (T_1, T_2, \dots, T_\ell)$  represents the set of patterns  $T_j$  applied at operating point  $OP_j$ ,  $j = 1, 2, \dots, \ell$ . Let  $N_j$  be the number of patterns in  $T_j$ .

Random testing of a circuit under multiple operating point  $OP^{(l)}$  consists of applying  $N_j$  patterns at operating point  $OP_j$ ,  $j = 1, 2, \dots, l$ .

Let  $F$  be the random variable representing the number of faults detected by a set of patterns  $T$  at an operating point  $OP$ . Let  $N$  be the number of patterns in  $T$ . Let  $p$  be the number of faults under consideration.

Definition 5.3:  $E\{F(N)\}$ , the expected number of fault detected by  $N$  patterns is given by

$$E\{F(N)\} = \sum_{i=1}^p i \cdot \Pr\{F=i\} = \sum_{i=1}^p i q_i$$

where  $F$  takes values  $i = 0, 1, \dots, p$  with probability  $q_i$ .

Example 5.1: Consider the circuit of Figure 5.1. Let the faults of interest be  $x_2$  s-a-0,  $x_2$  s-a-1,  $x_1$  s-a-0,  $x_1$  s-a-1,  $x_3$  s-a-0 and  $x_3$  s-a-1. We shall also refer to them as faults  $f_1, f_2, f_3, f_4, f_5$  and  $f_6$  respectively.

$$\Pr(\text{detecting } f_1 \text{ only}) = X_1 X_2 X_3$$

$$\Pr(\text{detecting } f_2 \text{ only}) = (1-X_2)(X_1 + X_3 - X_1 X_3)$$

$$\Pr(\text{detecting } f_i \text{ only}) = 0, i = 3, 4, 5, 6$$

$$\Pr(\text{detecting } f_1 \text{ and } f_3 \text{ only}) = X_1 X_2 (1-X_3)$$

$$\Pr(\text{detecting } f_1 \text{ and } f_5 \text{ only}) = (1-X_1) X_2 X_3$$

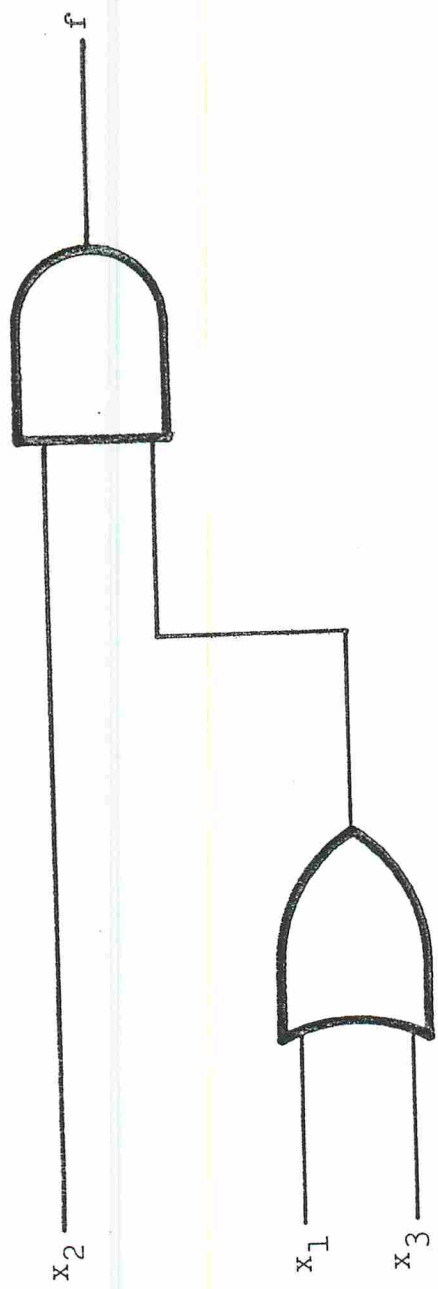


Figure 5.1. Circuit of Example 5.1



$$\Pr(\text{detecting } f_4 \text{ and } f_6 \text{ only}) = X_2(1-X_1)(1-X_3).$$

All other probabilities of detecting  $(f_j \text{ and } f_k \text{ only})$ ,  $j \neq k$  ( $f_j \text{ and } f_k \text{ and } f_l \text{ only}$ ),  $j \neq k \neq l$ , etc., are equal to zero.

$$\begin{aligned} E\{F(N)\} &= \sum_{i=1}^6 i \Pr(F=i) \\ &= 1 \cdot [1 - (1-X_1X_2X_3 - (1-X_2)(X_1+X_3-X_1X_3))^N] \\ &= 2 \cdot [1 - X_1X_2(1-X_3) - (1-X_1)(X_2X_3) \\ &\quad - X_2(1-X_1)(1-X_3))^N]. \end{aligned}$$

In general, to compute  $E\{F(N)\}$  one must compute  $2^p$  probability expressions if there are  $p$  faults in the circuit. If we assume that the complexity of computing a probability expression is  $O(E)$ , then computing  $E\{F(N)\}$  is  $O(2^p \cdot E)$ .

Definition 5.4 [SM75]: The error latency  $EL_i$  of a fault  $f_i$  is the number of input patterns applied to a circuit while  $f_i$  is present until the first incorrect output vector due to  $f_i$  is observed.

Definition 5.5 [SM75]: The quality  $Q_i(N)$  of a random test of length  $N$  for fault  $f_i$  is equal to the  $\Pr[EL_i \leq N]$ .

Definition 5.6: The average quality  $Q_{avg}(N)$  of a random test of length  $N$  over a set of faults  $f_1, f_2, \dots, f_p$  is given by

$$Q_{avg}(N) = \sum_{i=1}^p p_i \Pr[EL_i \leq N] = \sum_{i=1}^p p_i Q_i(N),$$



where  $p_i$  is the probability of occurrence of  $f_i$ .

Theorem 5.1: The functions  $Q_{avg}(N)$  and  $PD_{avg}(N)$  are equivalent.

Proof:

$$\begin{aligned}
 Q_{avg}(N) &= \sum_{i=1}^p p_i \cdot \Pr[EL_i \leq N] \\
 &= \sum_{i=1}^p p_i \cdot [1 - (1 - PD(f_i, 1))^N].
 \end{aligned}$$

From Section 3.4.1, we recall

$$\begin{aligned}
 PD_{avg}(N) &= \sum_{i=1}^p p_i \cdot PD(f_i, N) \\
 &= \sum_{i=1}^p p_i \cdot [1 - (1 - PD(f_i, 1))^N].
 \end{aligned}$$

Theorem 5.2: If all faults are equiprobable with  $p_i = \frac{1}{p}$ , then  $PD_{avg}(N) = \frac{1}{p} \cdot \sum_i PD(f_i, N) = \frac{1}{p} \cdot E\{F(N)\}$ .

Proof: Since  $p_i = \frac{1}{p}$

$$\begin{aligned}
 PD_{avg}(N) &= \sum_i \frac{1}{p} \cdot PD(f_i, N) \\
 &= \frac{1}{p} \sum_i PD(f_i, N).
 \end{aligned} \tag{5.1}$$

Consider a component  $PD(f_i, N)$  of the expression (5.1). We can write

$$\begin{aligned}
PD(f_1, N) = & \Pr(f_1, \bar{f}_2, \dots, \bar{f}_p, N) + \Pr(f_1, f_2, \bar{f}_3, \dots, \bar{f}_p, N) \\
& + \Pr(f_1, \bar{f}_2, f_3, \bar{f}_4, \dots, \bar{f}_p, N) + \dots \\
& + \Pr(f_1, \bar{f}_2, \bar{f}_3, \dots, \bar{f}_{p-1}, f_p, N) + \dots \\
& + \Pr(f_1, f_2, f_3, \bar{f}_4, \dots, \bar{f}_p, N) + \dots \\
& + \Pr(f_1, f_2, f_3, f_4, \bar{f}_5, \dots, \bar{f}_p, N) + \dots \\
& + \Pr(f_1, f_2, \dots, f_p, N)
\end{aligned} \tag{5.2}$$

where

$$\Pr(f_1^i, f_2^i, \dots, f_n^i, 1)$$

is given by

$$\bigcap_{j \in J} PD(f_j, 1) \quad \bigcap_{k \in K} [1 - PD(f_k, 1)] .$$

such that  $f_j^i = f_j$                       such that  $f_k^i = \bar{f}_k$

It should be noted that

$$\Pr(f_1^i, f_2^i, \dots, f_p^i, N) = 1 - [1 - \Pr(f_1^i, f_2^i, \dots, f_p^i, 1)]^N .$$

The components of the form

$$\Pr(\bar{f}_1, \bar{f}_2, \dots, \bar{f}_{i-1}, f_i, \bar{f}_{i+1}, \dots, \bar{f}_{j-1}, f_j, \bar{f}_{j+1}, \dots, \bar{f}_p, N)$$

appear in the expression for  $\sum_i PD(f_i, N)$ ,  $2 \cdot (n_{c_2})$  times and

$$\begin{aligned}
\sum \Pr(\bar{f}_1, \bar{f}_2, \dots, \bar{f}_{i-1}, f_i, \bar{f}_{i+1}, \dots, \bar{f}_{j-1}, f_j, \bar{f}_{j+1}, \dots, \bar{f}_p, N) \\
= 2\Pr[F = 2] .
\end{aligned}$$

From a similar analysis we can show

$$\begin{aligned} \sum \Pr(\bar{f}_1, \bar{f}_2, \dots, \bar{f}_{i-1}, f_i, \bar{f}_{i+1}, \dots, \bar{f}_{j-1}, f_j, \bar{f}_{j+1}, \dots, \bar{f}_{k-1}, \\ f_k, \bar{f}_{k+1}, \dots, \bar{f}_p, N) \\ = 3 \cdot \Pr[F = 3] \end{aligned}$$

and so on.

Hence we have

$$\sum_i \text{PD}(f_i, N) = \sum_i i \Pr\{F = i\}.$$

Hence

$$\text{PD}_{\text{avg}}(N) = \frac{1}{p} \cdot \sum_i \text{PD}(f_i, N) = \frac{1}{p} E\{F(N)\}. \quad \blacksquare$$

We have thus established the relationship between the two functions,  $\text{PD}_{\text{avg}}(N)$ , the average probability of detection and  $E\{F(N)\}$ , the expected number of faults detected under the condition that all faults are equiprobable.

Theorem 5.2 is not valid when the probability of occurrence of  $f_i$ ,  $i=1,2,\dots,p$  are not equal.

The complexity of computing the expression  $\text{PD}_{\text{avg}}(N)$  is  $O(p \cdot E)$  where  $p$  is the number of faults and the complexity of computing a probability expression is  $O(E)$ . Recall that the complexity of computing  $E\{F(N)\}$  is  $O(2^p E)$ .

### 5.3 Theory of Multiple Operating Point Random Testing

In this section we present the basic theory concerning multiple operating point random testing.

Let  $N$  be the total number of patterns to be applied. We will be concerned with maximizing the function  $PD_{avg}(N)$  (or equivalently  $Q_{avg}(N)$  or  $E\{F(N)\}$ ) by determining the input probability distribution at each operating point  $OP_j$ .

Example 5.2: Consider the NAND gate of Figure 5.2. All s-a-0, s-a-1 faults are assumed to be equally probable.

The probabilities of detecting  $x_1$  s-a-0 ( $x_2$  s-a-0,  $x_3$  s-a-1),  $x_1$  s-a-1,  $x_2$  s-a-1 and  $x_3$  s-a-0 are given by  $X_1X_2$ ,  $(1-X_1)X_2$ ,  $X_1(1-X_2)$  and  $(1-X_1X_2)$  respectively. For  $N=2$ , one of the optimal input distributions that maximizes  $p \cdot PD_{avg}(2)$  is given by  $X_1 = 1.0$  and  $X_2 = 0.6$ .  $p \cdot PD_{avg}(2)$  equals 3.80.

Consider a 2 operating point random test denoted by  $OP^{(2)} = (OP_1, OP_2)$  where  $OP_1 = (X_{11}, X_{21}) = (0, 1)$  and  $OP_2 = (X_{12}, X_{22}) = (1, 1)$ . Applying one pattern at each operating point of  $OP^{(2)}$  yields  $p \cdot PD_{avg}(2) = 5.0$ . We thus see that  $p \cdot PD_{avg}(2)$  under  $OP^{(2)}$  is greater than  $p \cdot PD_{avg}(2)$  under any  $OP^{(1)}$ .

Theorem 5.3: Let  $\ell$  and  $N$  represent the number of operating points and the number of input patterns applied.

1. The condition  $\ell > N$  is impossible.
2. The condition  $\ell = N$  implies that the best test set is a deterministic test set.

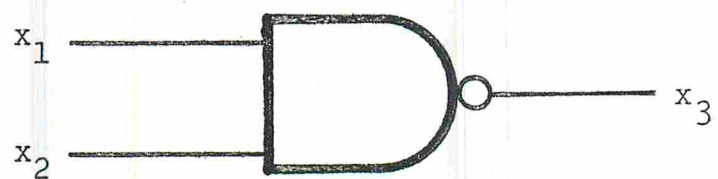


Figure 5.2. Circuit of Example 5.2

Proof: Since at least one pattern is applied at each operating point, the condition  $\ell > N$  is impossible.

The condition  $\ell = N$  implies that we apply only one vector at each operating point. If randomly generated patterns are applied at each of the operating points, then the same pattern may be applied at different operating points. Hence a deterministic test set is the best test set. ■ ■

It can be seen from Theorem 5.3 that only the condition  $\ell < N$  is of interest in multiple operating point random testing. It is clear that the upper bound on  $\ell$ , the number of operating points, is determined by the cardinality of a complete and minimal detection test set.

Theorem 5.4: For  $\ell, \ell' < N$ , there exists an  $\hat{OP}^{(\ell)}$  such that

$$PD_{avg}^{(N)} \Big|_{\hat{OP}^{(\ell)}} \cong PD_{avg}^{(N)} \Big|_{\hat{OP}^{(\ell')}} \quad (5.4)$$

for every  $\ell' < \ell$ .

Proof: Without loss of generality assume  $\ell - \ell' = 1$ . Assume that there exists no  $\hat{OP}^{(\ell)}$  such that

$$PD_{avg}^{(N)} \Big|_{\hat{OP}^{(\ell)}} \cong PD_{avg}^{(N)} \Big|_{\hat{OP}^{(\ell-1)}} \quad (5.5)$$

This implies that

$$PD_{avg}^{(N)} \Big|_{\hat{OP}^{(\ell)}} < PD_{avg}^{(N)} \Big|_{\hat{OP}^{(\ell-1)}} \quad (5.6)$$



Let  $\hat{OP}^{(\ell-1)} = (\hat{OP}_1, \hat{OP}_2, \dots, \hat{OP}_{\ell-1})$ .  $\hat{N}_i$  denotes the number of patterns applied at  $\hat{OP}_i$ ,  $i = 1, 2, \dots, \ell-1$ . Since  $\ell' < N$  there exists an  $\hat{N}_k > 1$ ,  $1 \leq k \leq \ell-1$ .

Create  $OP^{(\ell)}$  from  $\hat{OP}^{(\ell-1)}$  such that  $OP^{(\ell)} = (OP_1, OP_2, \dots, OP_k, \dots, OP_{\ell-1}, OP_\ell)$  such that

$$OP_i = \hat{OP}_i \quad 1 \leq i \leq \ell-1$$

$$OP_\ell = \hat{OP}_k \quad 1 \leq k \leq \ell-1.$$

Let  $N_i$  be the number of patterns applied at  $OP_i$ ,  $1 \leq i \leq \ell$ .

Let  $N_\ell = 1$

$$N_k = \hat{N}_k - 1$$

$$N_i = \hat{N}_i \quad \forall i \in \{1, 2, \dots, \ell-1\} - \{k\}.$$

Hence

$$\sum_{i=1}^{\ell} N_i = \sum_{j=1}^{\ell-1} \hat{N}_j = N.$$

Then

$$PD_{avg}^{(N)} \Big|_{OP^{(\ell)}} = PD_{avg}^{(N)} \Big|_{\hat{OP}^{(\ell-1)}},$$

thus contradicting our assumption. ■ ■

Theorem 5.5: Let  $OP^{(1)}(N)$  be an optimal single operating point for a circuit  $C$  when  $N$  random patterns are applied. Consider  $OP^{(2)}(N) = (OP_1, OP_2)$  for the circuit  $C$ . Let  $a_i'$ ,  $a_{i1}$ ,  $a_{i2}$  be the probabilities of detecting  $f_i$  at  $OP^{(1)}$ ,  $OP_1$ ,

$OP_2$  respectively, and  $N_1 + N_2 = N$ .

If  $(1-a'_i)^N > (1-a_{i1})^{N_1}(1-a_{i2})^{N_2}$  for every  $f_i$ , then

$$PD_{avg}^{(N)} \Big|_{OP^{(2)}(N)} > PD_{avg}^{(N)} \Big|_{OP^{(1)}(N)}.$$

Proof: For simplicity we denote  $OP^{(1)}(N)$  and  $OP^{(2)}(N)$  by  $OP^{(1)}$  and  $OP^{(2)}$  respectively.

$$\begin{aligned} PD_{avg}^{(N)} \Big|_{OP^{(1)}} &= \sum_i p_i \cdot PD(f_i, N) \\ &= \sum_i p_i [1 - (1 - PD(f_i, 1))^N] \\ &= \sum_i p_i [1 - (1 - a'_i)^N] \end{aligned}$$

$$\begin{aligned} PD_{avg}^{(N)} \Big|_{OP^{(2)}} &= \sum_i p_i PD(f_i, N) \\ &= \sum_i p_i [1 - (1 - a_{i1})^{N_1} (1 - a_{i2})^{N_2}]. \end{aligned}$$

Since  $(1-a'_i)^N > (1-a_{i1})^{N_1}(1-a_{i2})^{N_2}$  for every  $i$ ,  $1 - (1-a'_i)^N < 1 - (1-a_{i1})^{N_1}(1-a_{i2})^{N_2}$  and hence

$$PD_{avg}^{(N)} \Big|_{OP^{(2)}} > PD_{avg}^{(N)} \Big|_{OP^{(1)}}. \quad (5.3)$$

If  $N_1 = N_2 = N/2$ , the sufficient condition is given by

$$(1-a_i)^2 > (1-a_{i1})(1-a_{i2}).$$

In general, we have the following theorem.

Theorem 5.6:  $PD_{avg}(N) \Big|_{OP(m)} > PD_{avg}(N) \Big|_{OP(1)}$  for a circuit C if  $(1-a'_i)^N > (1-a_{i1})^{N_1}(1-a_{i2})^{N_2} \dots (1-a_{im})^{N_m} \forall i$  where  $N_1 + N_2 + \dots + N_m = N$  and  $a_{i1}, a_{i2}, \dots, a_{im}$  are the probabilities of detecting  $f_i$  at  $OP_1, OP_2, \dots, OP_m$  respectively. ■■

Also, if  $N_1, N_2, \dots, N_m = N/m$ , this condition reduces to  $(1-a'_i)^m > (1-a_{i1})(1-a_{i2}) \dots (1-a_{im})$ .

We will now present a procedure for the generation of optimal multiple operating points, given  $N$ , the total number of input patterns and  $\ell$ , the number of operating points.

$PD_j(f_k, N_j)$  denotes the probability of detecting  $f_k$  at operating point  $OP_j$  by the application of  $N_j$  patterns.

$PND_j(f_k, N_j)$  denotes the expression  $1 - PD_j(f_k, N_j)$ .

Procedure 5.1:

1. Compute the probability expression for detecting fault  $f_k$ ,  $k = 1, 2, \dots, p$ .
2. Derive the expression

$$PND(f_k) \Big|_{OP(\ell)} \triangleq \prod_{j=1}^{\ell} PND_j(f_k, N_j).$$

$$3. \quad \beta = \sum_{k=1}^p \left( 1 - PND(f_k) \Big|_{OP(\ell)} \right). \quad (5.4)$$

4. Maximize  $\beta$  such that

$$0 \leq X_{ij} \leq 1 \quad \begin{array}{l} i = 1, 2, \dots, n \\ j = 1, 2, \dots, \ell \end{array}$$

where  $X_{ij} = \Pr(x_i = 1) \text{ at } OP_j$ .

It has been shown in Chapter 3 that the problem of maximizing Eq.(5.4) is a complex numerical analysis problem.

Example 5.3: Consider the circuit of Figure 5.3. All faults are assumed to be equally probable.

Tables 5.1 and 5.2 are results obtained during a fine grid search of grid size equal to  $1/15$  when only one operating point is considered. Table 5.1 shows the maximum  $p \cdot PD_{avg}(N)$  and minimum  $p \cdot PD_{avg}(N)$  and the associated input probability distributions for  $N = 2, 4, 6, 8$ .

Table 5.2 shows the number of input probability distributions having  $\lfloor p \cdot PD_{avg}(N) \rfloor = 0, 1, 2, \dots, 10$ .

Tables 5.3 and 5.4 are results obtained using the grid search procedure when two operating points are considered. Grid size was restricted to  $1/3$  in order to keep the total number of input probability distributions the same under one and two operating points. Let

$$OP^{(2)} = (OP_1, OP_2)$$

where

$$OP_1 = (X_{11}, X_{21}, X_{31})$$

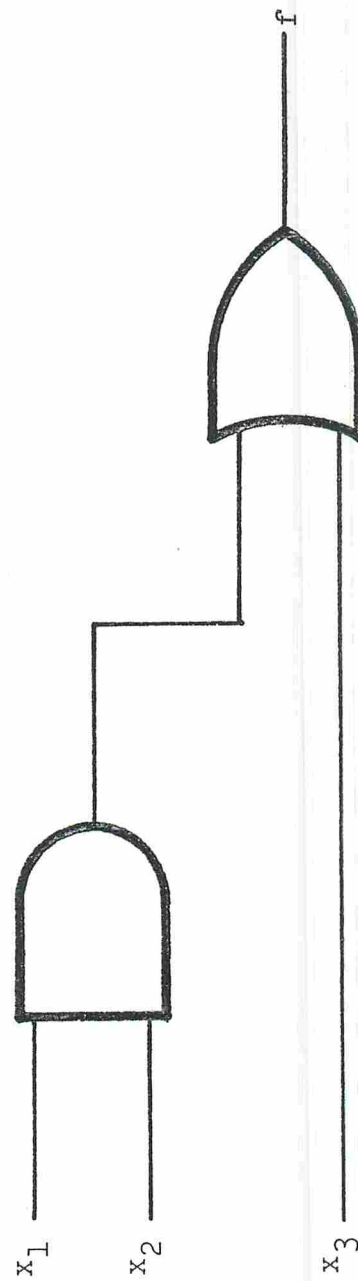


Figure 5.3. Circuit of Example 5.3

Table 5.1. Optimal and Worst Case Distributions Corresponding to Maximum  $p \cdot PD_{avg}$  and Minimum  $p \cdot PD_{avg}$  for  $N = 2, 4, 6, 8$  Under  $OP(1)$  for Example 5.3.

N	Type of Solution	$x_1$	$x_2$	$x_3$	$p \cdot PD_{avg}$
2	Optimal	0.933	0.533	0	5.998
	Worst	1	1	1	1
4	Optimal	0.733	.667	0	7.7727
	Worst	1	1	1	1
6	Optimal	.667	.667	.133	8.5829
	Worst	1	1	1	1
8	Optimal	.6	.6	.2	9.089
	Worst	1	1	1	1

Table 5.2. Number of Input Distributions and Associated  $\lfloor p \cdot PD_{avg}(N) \rfloor$  for  $N = 2, 4, 6, 8$  Under  $OP(1)$ .

$\lfloor p \cdot PD_{avg} \rfloor$	N = 2	N = 4	N = 6	N = 8
0	0	0	0	0
1	250	212	165	131
2	592	307	105	128
3	986	344	322	293
4	1550	745	453	346
5	718	1081	893	717
6	0	864	853	728
7	0	543	838	813
8	0	0	467	906
9	0	0	0	34
10	0	0	0	0



Table 5.3. Optimal and Worst Case Distributions  
for  $N = 2, 4, 6, 8$  Under  $OP^{(2)}$ .

N	Type of Solution	$X_{11}$	$X_{21}$	$X_{31}$	$X_{12}$	$X_{22}$	$X_{32}$	$p \cdot PD_{avg}$
2	Optimal	0	1	0	1	1	0	8.000
	Worst	1	1	1	1	1	1	1.000
4	Optimal	1	0.667	0	0	1	.333	8.469
	Worst	1	1	1	1	1	1	1.000
6	Optimal	1	0.667	0	0	1	.333	9.2153
	Worst	1	1	1	1	1	1	1.000
8	Optimal	1	0.667	0	0	1	.333	9.5458
	Worst	1	1	1	1	1	1	1.000

Table 5.4. Number of Input Distributions and the  
Associated  $\lfloor p \cdot PD_{avg} \rfloor$  Under  $OP^{(2)}$

$\lfloor p \cdot PD_{avg} \rfloor$	N = 2	N = 4	N = 6	N = 8
0	0	0	0	0
1	81	81	81	76
2	316	177	175	180
3	752	211	29	25
4	1411	571	611	275
5	1326	1279	777	1024
6	186	1023	922	443
7	20	714	925	917
8	4	40	568	1018
9	0	0	8	138
10	0	0	0	0

and

$$OP_2 = (X_{12}, X_{22}, X_{32}).$$

Since the grid size for  $OP^{(2)}$  is  $1/3$ , each  $X_{ij} \in \{0, 1/3, 2/3, 1\}$  where  $i \in \{1, 2, 3\}$  and  $j \in \{1, 2\}$ . Hence the number of input probability distributions under  $OP^{(2)}$  is given by  $4^6$ . Under  $OP^{(1)}$  the number of distributions with a grid size of  $1/15$  is given by  $16^3 = 4^6$ .

It should be noted that every possible operating point in  $OP^{(2)}$  exists in  $OP^{(1)}$ .

An equal number of vectors is applied at each of the operating points of  $OP^{(2)} = (OP_1, OP_2)$ .

From these results, we can make the following observations.

1. The maximum  $p \cdot PD_{avg}(N)$  increases with increasing  $N$  under  $OP^{(2)}$ .

2. From Tables 5.2 and 5.4, it can be seen that for  $\lfloor p \cdot PD_{avg}(N) \rfloor = 7, 8$ , and  $9$  there are many more input probability distributions under the two operating point random test than under the single operating point test for  $N = 6, 8$ . This seems to indicate that in general there are better chances of maximizing the expected number of faults detected under a two operating point random test.

3. Let  $N/2$  vectors be applied at each of the operating points of  $OP^{(2)}$ . Then the worst case distribution of

$OP^{(2)}$  for a given  $N$  is the same as the worst case distribution under  $OP^{(1)}$  for the same  $N$ .

#### 5.4 A Special Class of Input Probability Distributions

In this section we present results concerning a class of input probability distributions that have the property that, under these distributions, no two  $n$  variable combinational functions have the same output probability.

Theorem 5.7 [MPS78]: There exists a set of input probabilities  $X_1, X_2, \dots, X_1, \dots, X_n$  where

$$X_i = \frac{2^{2^{(n-i)}}}{2^{2^{(n-i)}} + 1}$$

so that no two  $n$  variable combinational functions have the same output probability  $Z$ .

Example 5.4: Consider  $n = 2$ .

$$X_1 = \Pr(x_1 = 1) = 4/5$$

$$X_2 = \Pr(x_2 = 1) = 2/3.$$

The probabilities of the 4 possible minterms are given by

$$M_0 = \Pr(\bar{x}_1 \bar{x}_2 = 1) = 1/15$$

$$M_1 = \Pr(\bar{x}_1 x_2 = 1) = 2/15$$

$$M_2 = \Pr(x_1 \bar{x}_2 = 1) = 4/15$$

$$M_3 = \Pr(x_1 x_2 = 1) = 8/15.$$

Table 5.5 shows the output probabilities of the 16 functions of two variables. Note that the output probabilities of the 16 functions of two variables are uniformly distributed over the interval  $[0,1]$ . It can be seen that the probability of a function  $f$  represented by  $[A_0 A_1 A_2 A_3]$  is given by  $\frac{D}{2^{2^n} - 1}$  where  $D$  is the integer corresponding to  $[A_3 A_2 A_1 A_0]$ .

In general the output probabilities of the  $2^{2^n}$  functions of  $n$  variables are uniformly distributed over the interval  $[0,1]$ .

Theorem 5.8: Let  $P(2;n) \triangleq \{G_1, G_2, \dots, G_n\}$  where  $G_i = \{G_{i0}, G_{i1}\}$   
 $G_{i0} = \frac{1}{2^{2^{(i-1)}} + 1}$  and  $G_{i1} = 1 - G_{i0}$ ,  $i = 1, 2, \dots, n$ . Let  $X = (X_1, X_2, \dots, X_n)$  be assigned values from a subset of  $P(2;n)$  such that only one element of every  $G_i$  is present in  $X$  and  $X_i \neq X_j$  for  $i \neq j$ . There are  $2^n \cdot n!$  possible assignments to  $X$  such that no two functions of  $n$  variables have the same output probability.

Proof: We first choose a  $G_i$  and then either  $G_{i0}$  or  $G_{i1}$  for  $X_1$ . There are  $2n$  ways of making this assignment. For  $X_2$  we first choose

$$G_j \in \{P(2;n)\} - \{G_i\}$$

Table 5.5. Output Probabilities of 16 Functions  
of 2 Variables

Function f in Terms of				Pr( $f = 1$ )
$A_0$	$A_1$	$A_2$	$A_3$	
0	0	0	0	0/15
0	0	0	1	8/15
0	0	1	0	4/15
0	0	1	1	12/15
0	1	0	0	2/15
0	1	0	1	10/15
0	1	1	0	6/15
0	1	1	1	14/15
1	0	0	0	1/15
1	0	0	1	9/15
1	0	1	0	5/15
1	0	1	1	13/15
1	1	0	0	3/15
1	1	0	1	11/15
1	1	1	0	7/15
1	1	1	1	15/15



and then  $X_2$  is assigned the value  $G_{j_1}$  or  $G_{j_2}$ . There are  $2(n-1)$  ways of making this assignment. This process is continued until  $X_n$  is assigned a value. Thus the total number of assignments is  $2n \cdot 2(n-1) \dots 2 \cdot 1 = 2^n \cdot n!$ .

Let the assignment relation be defined by

$$X_i = G_{T_i K_i}$$

where

$$T_i \in \{1, 2, \dots, n\} \quad \text{and} \quad K_i \in \{0, 1\}.$$

Let the  $n$  bit binary representation of the integer  $j$  be  $j_1, j_2, \dots, j_n$  where  $j_\ell \in \{0, 1\}$ .

$$\text{Let } \sigma_\ell = 2(1 - j_\ell - k_\ell + 2j_\ell k_\ell) \quad \forall \ell \in \{1, 2, \dots, n\}, \quad \sigma_\ell \in \{0, 2\}.$$

Then

$$\begin{aligned} M_j &= \frac{2^{\sigma_1 T_1} \cdot 2^{\sigma_2 T_2} \dots 2^{\sigma_n T_n}}{(2^{2^{T_1} + 1})(2^{2^{T_2} + 1}) \dots (2^{2^{T_n} + 1})} \\ &= \frac{E(j)}{D} \end{aligned}$$

where

$$E(j) = \prod_{\ell=1}^n 2^{\sigma_\ell T_\ell}$$

and

$$D = \prod_{\ell=1}^n (2^{2^{T_\ell} + 1}).$$



Let  $D_1$  and  $D_2$  be two subsets of  $D$  such that  $D_1 \neq D_2$ . It can be shown from number theory techniques that

$$\sum_{j \in D_1} E(j) \neq \sum_{j \in D_2} E(j).$$

Let  $f_1(2)$  be the function having the minterms  $m_j$  such that  $j \in D_1(2)$ . Then

$$\Pr(f_1=1) = \frac{\sum_{j \in D_1} E(j)}{D}$$

and

$$\Pr(f_2=1) = \frac{\sum_{j \in D_2} E(j)}{D}.$$

Since  $\sum_{j \in D_1} E(j) \neq \sum_{j \in D_2} E(j)$ ,

$$\Pr(f_1=1) \neq \Pr(f_2=1).$$

■ ■

We now give a more general form of the previous theorem.

Theorem 5.9: Let  $P(I;n) \triangleq \{G_1, G_2, \dots, G_n\}$ ,  $I = 2, 3, \dots$ , where  $G_i = \{G_{i0}, G_{i1}\}$ ,  $G_{i0} = \frac{1}{I^{2(i-1)} + 1}$  and  $G_{i1} = 1 - G_{i0}$ . Let  $X = (X_1, X_2, \dots, X_n)$  be assigned values from a subset of  $P(I;n)$  such that only one element of every  $G_i$  is present in  $X$  and  $X_i \neq X_j$  for  $i \neq j$ . No two  $n$  variable combinational functions

have the same output probability under X.

Proof: Without loss of generality, we assume

$$\begin{aligned} X_n &= \frac{1}{I^2 + 1} = \frac{1}{I+1} \quad \text{and} \quad 1-X_n = \frac{I}{I+1} \\ X_{n-1} &= \frac{1}{I^2 + 1} \quad \text{and} \quad 1-X_{n-1} = \frac{I^2}{I^2 + 1} \\ &\vdots \\ X_1 &= \frac{1}{I^{2^{(n-1)}} + 1} \quad \text{and} \quad 1-X_1 = \frac{I^{2^{(n-1)}}}{I^{2^{(n-1)}} + 1} . \end{aligned}$$

There are  $2^n$  possible minterms  $m_0, m_1, \dots, m_{2^n-1}$  and the corresponding probabilities are  $M_0, M_1, \dots, M_{2^n-1}$ . Let the  $n$  bit binary representation of  $i$  be  $i_1 i_2 \dots i_n$  where  $i_j \in \{0, 1\}$ .

Then

$$M_i = \frac{I^{(2-2i_1)^{n-1}} \cdot I^{(2-2i_2)^{n-2}} \dots I^{(2-2i_n)^0}}{(I^{2^{(n-1)}} + 1)(I^{2^{(n-2)}} + 1) \dots (I^2 + 1)(I + 1)} ,$$

$$i = 0, 1, \dots, 2^n - 1 . \quad (5.5)$$

Let the numerator of (5.5) be  $E(i)$ . Consider two subsets  $D_1$  and  $D_2$  of the set  $\{0, 1, \dots, 2^n - 1\}$  such that  $D_1 \neq D_2$ .

It can be shown from number theory techniques that

$$\sum_{i \in D_1} E(i) \neq \sum_{j \in D_2} E(j) .$$

Let  $f_1$  be the function having all the minterms  $m_i$  such that  $i \in D_1$  and  $f_2$  be the function having all the minterms  $m_j$

such that  $j \in D_2$ . Then

$$\Pr(f_1=1) = \frac{\sum_{i \in D_1} E(i)}{(I+1)(I^2+1) \dots (I^{2^{(n-1)}}+1)}$$

and

$$\Pr(f_2=1) = \frac{\sum_{j \in D_2} E(j)}{(I+1)(I^2+1) \dots (I^{2^{(n-1)}}+1)}.$$

Therefore  $\Pr(f_1=1) \neq \Pr(f_2=1)$ . ■ ■

The following results can be easily proved.

1. The input probability distribution given by

$$\hat{X} = \left( 1 - \frac{1}{I^{2^{(n-1)}}+1}, 1 - \frac{1}{I^{2^{(n-2)}}+1}, \dots, 1 - \frac{1}{I^{2^0}+1} \right)$$

generates the condition  $M_i = \frac{I^i}{D}$ ,  $i = 0, 1, \dots, 2^n - 1$ . Hence under  $\hat{X}$ ,  $M_i > M_j$  for  $i > j$ .

2. The input probability distribution given by

$$\hat{X} = \left( \frac{1}{I^{2^{(n-1)}}+1}, \frac{1}{I^{2^{(n-2)}}+1}, \dots, \frac{1}{I^{2^0}+1} \right)$$

generates the condition  $M_i = \frac{I^{2^n-1-i}}{D}$ ,  $i = 0, 1, \dots, 2^n - 1$ .

Under  $\hat{X}$ ,  $M_i > M_j$  for  $i < j$ .

3. Let  $M_i | X$  denote the probability of minterm  $m_i$  being one under the distribution  $X$ .

There are  $2^n$  probability distributions  $X(1), X(2), \dots, X(2^n)$  given by the relationship

$$\begin{aligned} X_n &= \left( 1 - \frac{1}{I^{2^0} + 1} \right) \text{ or } \left( \frac{1}{I^{2^0} + 1} \right) \\ X_{n-1} &= \left( 1 - \frac{1}{I^{2^1} + 1} \right) \text{ or } \left( \frac{1}{I^{2^1} + 1} \right) \\ &\vdots \\ X_1 &= \left( 1 - \frac{1}{I^{2^{(n-1)}} + 1} \right) \text{ or } \left( \frac{1}{I^{2^{(n-1)}} + 1} \right) \end{aligned}$$

such that

$$\left\{ M_i |_{X(1)}, M_i |_{X(2)}, \dots, M_i |_{X(2^n)} \right\} = \left\{ \frac{I^0}{D}, \frac{I^1}{D}, \dots, \frac{I^{2^n-1}}{D} \right\}.$$

Example 5.5: Let  $n=2$ ,  $I=3$ . Under  $\hat{X}$ ,  $X_1 = \frac{1}{10}$  and  $X_2 = \frac{1}{4}$ . The probabilities of the four possible minterms are

$$M_0 = \Pr(\bar{x}_1 \bar{x}_2 = 1) = \frac{27}{40}$$

$$M_1 = \Pr(\bar{x}_1 x_2 = 1) = \frac{9}{40}$$

$$M_2 = \Pr(x_1 \bar{x}_2 = 1) = \frac{3}{40}$$

$$M_3 = \Pr(x_1 x_2 = 1) = \frac{1}{40}.$$

The output probabilities of the 16 functions of 2 variables are shown in Table 5.6.

Table 5.6. Output Probabilities of the 16 Functions of 2 Variables Under  $P(3;2)$ .

Function F in Terms of				Pr(f=1)
$A_0$	$A_1$	$A_2$	$A_3$	
0	0	0	0	0/40
0	0	0	1	1/40
0	0	1	0	3/40
0	0	1	1	4/40
0	1	0	0	9/40
0	1	0	1	10/40
0	1	1	0	12/40
0	1	1	1	13/40
1	0	0	0	27/40
1	0	0	1	28/40
1	0	1	0	30/40
1	0	1	1	31/40
1	1	0	0	36/40
1	1	0	1	37/40
1	1	1	0	39/40
1	1	1	1	40/40



Example 5.6: Let  $n=2$ ,  $I=4$ . Under  $\hat{X}$ , we have  $X_1 = \frac{1}{17}$  and  $X_2 = \frac{1}{5}$ .

$$M_0 = \frac{64}{85}, \quad M_1 = \frac{16}{85}, \quad M_2 = \frac{4}{85}, \quad \text{and} \quad M_3 = \frac{1}{85}.$$

The output probabilities are shown in Table 5.7.

It can be seen from Examples 5.4, 5.5, and 5.6 that a uniform distribution of output probabilities occurs for  $I=2$ . Under  $\hat{X}$ , for  $I>2$ , the output probabilities tend to cluster into two groups, one group consisting of terms where  $A_0 = 0$  and the other where  $A_0 = 1$ , that grow farther apart as  $I$  increases.

For  $I=3,4$  the minimum difference between the output probabilities of the two groups is  $\frac{14}{40}$  and  $\frac{43}{85}$  respectively.

### 5.5 Concluding Remarks

In this chapter we have introduced the concept of multiple operating point random testing of digital circuits. We have shown that this concept is of interest only when  $\ell$ , the number of operating points is less than  $N$ , the number of patterns to be applied. The existence of multiple operating points of cardinality  $< N$  such that  $PD_{avg}^{(N)} \Big|_{\hat{OP}(\ell)} \cong PD_{avg}^{(N)} \Big|_{\hat{OP}(\ell')}$  for every  $\ell' < \ell$  has been shown. It is an open question whether these operating points are all unique for every circuit  $C$ , given  $1 < \ell < N$  and  $N \geq 3$ .



Table 5.7. Output Probabilities of the 16 Functions of 2 Variables Under  $P(4;2)$

Function F in Terms of				Pr(f = 1)
$A_0$	$A_1$	$A_2$	$A_3$	
0	0	0	0	0/85
0	0	0	1	1/85
0	0	1	0	4/85
0	0	1	1	5/85
0	1	0	0	16/85
0	1	0	1	17/85
0	1	1	0	20/85
0	1	1	1	21/85
1	0	0	0	64/85
1	0	0	1	65/85
1	0	1	0	68/85
1	0	1	1	69/85
1	1	0	0	80/85
1	1	0	1	81/85
1	1	1	0	84/85
1	1	1	1	85/85

In addition, we have presented a class of input probability distributions with the property that no two  $n$  variable functions have the same output probability under these distributions.

## CHAPTER 6

### CONCLUDING REMARKS

We have presented a transform technique to characterize the behavior of digital circuits under random inputs. It has been shown that this transform is closely related to other transforms, such as the RMC and the Walsh transforms, used in the design and analysis of digital circuits. The row vectors of the matrix  $P$  form a basis for a probability expression  $F(X_1, X_2, \dots, X_n)$  of a Boolean function  $f(x_1, x_2, \dots, x_n)$ . Further investigation is necessary to characterize the class of matrices that form a basis for the Boolean function  $f$ . It is hoped that a generalized transform technique for the analysis, design and testing of digital circuits will incorporate existing transform techniques as special cases.

We have shown that the expression  $\frac{\partial F}{\partial X_1}$  is a tool for both deterministic and random test generation. The computation of the optimal input distributions for generating "effective" random input patterns is not feasible for big circuits using the fine grid search or the variable metric method. Further work needs to be done in finding good techniques to find the global maxima of the expression  $\beta$

(Eq. 3.5) and the associated optimal input probabilities.

A matrix model of the form  $L^T(\underline{Y}^+) = C(\underline{X})L^T(\underline{Y}) + E$  has been presented to analyze the behavior of a synchronous sequential circuit under random inputs. Probabilistic synchronization has been shown to be related to the spectral radius of the matrix  $C(\underline{X})$ . Further investigation is needed for efficiently computing the input probability distribution which yields the smallest spectral radius, since it is this distribution which gives the quickest possible probabilistic synchronization.

Another unsolved problem consists of determining other aspects of the behavior of synchronous sequential circuits such as the construction of distinguishing sequences (when they exist) and homing sequences by studying the properties of the associated matrix  $C(\underline{X})$ . It would also be interesting to determine the class of sequential circuits that have the following property:

1. the associated matrix  $C(\underline{X})$  is symmetric.
2. the eigenvalues of the associated matrix  $C(\underline{X})$  are all real.

The concept of multiple operating point random testing has been introduced. It is shown that using this concept the effectiveness of testing digital circuits can be improved. An open question is the uniqueness properties of  $OP^{(\ell)}$  for different  $\ell$  given  $1 < \ell < N$  and  $N \geq 3$  for any cir-

cuit C.

A class of input probability distributions  $P(I;n)$  with the property that under  $P(I;n)$  no two  $n$ -variable Boolean functions have the same output probability has been presented.

These distributions are of practical interest because they can be used to predict the output response of fault free and faulty functions. Further research in this area is necessary in order to determine how these distributions can best be used in the testing of circuits.



## REFERENCES

- [AA72] Agrawal, V.D. and P. Agrawal, "An automatic test generation system for Illiac IV logic boards," *IEEE Trans. Computers*, vol. C-21, pp. 1015-1017, September 1972.
- [AA75a] Agrawal, P. and V.D. Agrawal, "Probabilistic analysis of random test generation method for irredundant combinational logic networks," *IEEE Trans. Computers*, vol. C-24, pp. 691-695, June 1975.
- [AA75b] Agrawal, P and V.D. Agrawal, "On improving the efficiency of Monte Carlo test generation," *Proc. International Symposium on Fault Tolerant Computing*, Paris, France, pp. 205-209, June 1975.
- [AA76] Agrawal, P. and V.D. Agrawal, "On Monte Carlo testing of logic tree networks," *IEEE Trans. Computers*, vol. C-25, pp. 664-669, June 1976.
- [AHU74] Aho, A.V., Hopcroft, J.E., and J.D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison Wesley Publishing Company, 1974.
- [Ar66] Armstrong, D.B., "On finding a nearly minimal set of fault detection tests for combinational logic nets," *IEEE Trans. Computers*, vol. EC-15, pp. 66-73, February 1966.
- [BD62] Bellman, R. and D. Dreyfuss, *Applied Dynamic Programming*, Princeton University Press, Princeton N.J., 1962.
- [Be71] Betancourt, R., "Derivation of minimum test sets for unate logical circuits," *IEEE Trans. Computers*, vol. C-20, pp. 1264-1269, 1971.
- [BH69] Ball, M. and F. Hardie, "Effects and detection of intermittent failures in digital systems," *Proc. 1969 Fall Joint Computer Conf.*, pp. 329-335, 1969.



- [Hu73] Hurst, S.L., "Application of Chow parameters and Rademacher-Walsh matrices in the synthesis of binary functions," *Comp. Journal*, vol. 16, pp. 165-173, 1973.
- [Hu77] Hurst, S.L., "Detection of symmetries in combinatorial functions by spectral means," *IEEE J. Electronic Circuits and Systems*, vol. 1, pp. 173-180, 1977.
- [Ko77] Koren, I., "Signal reliability of combinational and sequential circuits," *Proc. 7th International Conference on Fault Tolerant Computing*, pp. 162-167, June 1977.
- [KP74] Kamal, S. and C.V. Page, "Intermittent faults: a model and detection procedure," *IEEE Trans. Computers*, vol. C-23, pp. 713-719, June 1974.
- [KS60] Kemeny, J. and J. Snell, *Finite Markov Chains*, Van Nostrand, Princeton, N.J., 1960.
- [Le71] Lechner, R.J., in *Recent Developments in Switching Theory*, (A. Mukhopadhyay, ed.), Academic Press, New York, 1971.
- [Lo77] Losq, J., "Efficiency of compact testing for sequential circuits," *Proc. Fault Tolerant Computing Conference*, pp. 168-174, June 1977.
- [Ma77] Marouf, M.A., "Design of Self-Checking Checkers and Easily Testable Circuits," Ph.D. Dissertation, University of Southern California, August 1977.
- [MH78] Muzio, J.C. and S.L. Hurst, "The computation of complete and reduced sets of orthogonal spectral coefficients for logic design and pattern recognition purposes," *Comput. and Electrical Engineering*, vol. 5, pp. 231-249, 1978.
- [MPS78] McCluskey, E.J., Parker, K.P., and J.J. Shedletsky, "Boolean network probabilities and network design," *IEEE Trans. Computers*, vol. C-27, pp. 187-189, February 1978.
- [MS70] Mukhopadhyay, A. and G. Schmitz, "Minimization of Exclusive-OR and logical equivalence switching circuits," *IEEE Trans. Computers*, vol. C-19,

pp.132-140, February 1970.

- [PM75a] Parker, K.P. and E.J. McCluskey, "Probabilistic treatment of general combinational networks," *IEEE Trans. Computers*, vol. C-24, pp. 668-670, June 1975.
- [PM75b] Parker, K.P. and E.J. McCluskey, "Analysis of logic circuits with faults using input signal probabilities," *IEEE Trans. Computers*, vol. C-24, pp. 573-578, May 1975.
- [Po63] Poage, J.F., "Derivation of optimum tests to detect faults in combinational circuits," *Proc. Symposium on Mathematical Theory of Automata*, pp. 483-528, 1963.
- [Pa69] Papoulis, A., *Probability, random variable, and stochastic processes*, McGraw-Hill Book Company, New York, 1969.
- [Pr64] Preparata, F.P., "State logic relations for autonomous sequential circuits," *IEEE Trans. Computers*, vol. EC-13, pp. 542-548, October 1964.
- [Ra71] Rault, J.C., "A graph-theoretic and probabilistic approach to fault detection of digital circuits," *Digest Int'l. Symposium Fault Tolerant Computing*, pp. 26-29, March 1971.
- [Ro66] Roth, J.P., "Diagnosis of automata failures: a calculus and a method," *IBM Journal of Research and Development*, vol. 10, pp. 278-291, July 1966.
- [Sa77] Savir, J., "Detection of Intermittent Failures in Combinational Cricuits," Tech. Report 120, Digital Systems Laboratory, Stanford University, Stanford, California, July 1977.
- [Sh69] Shanks, J., "Computation of the fast Walsh-Fourier transform," *IEEE Trans. Computers*, vol. EC-18, pp. 457-459, 1969.
- [SHB68] Sellers, F.F., Hsiao, M.Y., and C.L. Bearnson, "Analyzing errors with the Boolean difference," *IEEE Trans. Computers*, vol. C-17, pp. 676-683, July 1968.

- [SLC75] Schnurmann, H.D., Lindbloom, E., and R.G. Carpenter, "The weighted random test pattern generator," *IEEE Trans. Computers*, vol. C-24, pp. 695-700, July 1975.
- [SKM78] Su, S.Y.H., Koren, I., and Y.K. Malaiya, "A continuous parameter Markov model and detection procedure for intermittent faults," *IEEE Trans. Computers*, vol. C-27, pp. 567-570, June 1978.
- [SM75] Shedletsky, J.J. and E.J. McCluskey, "The error latency of a fault in a combinational digital circuit," *Digest 1975 Int'l. Symposium Fault Tolerant Computing*, Paris, France, pp. 210-214, June 1975.
- [SM76] Shedletsky, J.J. and E.J. McCluskey, "The error latency of a fault in a sequential circuit," *IEEE Trans. Computers*, vol. C-25, pp. 655-659, June 1976.
- [S079] Saluja, K.K. and E.H. Ong, "Minimization of Reed-Muller canonic expansion," *IEEE Trans. Computers*, vol. C-28, pp. 535-537, July 1979.
- [Sw72] Swamy, S., "On generalized Reed-Muller expansions," *IEEE Trans. Computers*, vol. C-21, pp. 1008-1009, 1972.
- [Wa23] Walsh, J.L., "A closed set of orthogonal functions," *American J. Math.*, vol. 45, pp. 5-24, 1923.



## APPENDIX

### REED-MULLER FORM OF SEQUENTIAL CIRCUITS

Theorem A.1: Let  $r'_{ij}(\underline{x}) = \bigoplus_{t \in N_j} |e_{it}|_{\text{mod } 2} \ell_t(\underline{x})$  where  $d_{ij}(\underline{x}) = \sum_{t \in N_j} e_{it} \ell_t(\underline{x})$  and  $\bigoplus$  denotes mod 2 addition. Construct the elements  $r_{ij}(\underline{x})$  of the matrix  $R(\underline{x})$  from  $r'_{ij}(\underline{x})$  by replacing  $\underline{x}$  in  $r'_{ij}$  by  $\underline{\bar{x}}$ . Then  $B^T(\underline{y}^+) = R(\underline{\bar{x}})B^T(\underline{y})$  over  $\text{GF}(2)$ .

Proof: Consider  $B(\underline{y}^+; i)$ , the  $i^{th}$  component of  $B(\underline{y}^+)$ .

$$\begin{aligned} B(\underline{y}^+; i) &= \sum_{j=1}^{2^n} d_{ij}(\underline{x}) B(\underline{y}; j) \\ &= \sum_{j=1}^{2^n} \sum_{t \in N_j} e_{it} \ell_t(\underline{x}) B(\underline{y}; j). \end{aligned}$$

From Theorem 2.13 we know that the RMC coefficients of  $B(\underline{y}^+; i)$  are obtained by taking  $|e_{it}|_{\text{mod } 2}$  for every  $t$ . Hence the RMC expression for  $B(\underline{y}^+; i)$  is given by

$$\begin{aligned} B(\underline{y}^+; i) &= \bigoplus_{j=1}^{2^n} \bigoplus_{t \in N_j} |e_{it}|_{\text{mod } 2} \ell_t(\underline{x}) B(\underline{y}; j) \\ &= \bigoplus_{j=1}^{2^n} r_{ij}(\underline{x}) B(\underline{y}; j). \end{aligned}$$

Therefore

$$B^T(\underline{y}^+) = R(\underline{x})B^T(\underline{y}) \text{ over GF}(2).$$

Example A.1: Consider the sequential circuit of Example 4.3. We have shown that this circuit can be represented by

$$B^T(\underline{y}^+) = D(\underline{X})B^T(\underline{y})$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & (1+X) & 0 & -X \\ 0 & 1 & 0 & (-1+X) \\ 0 & X & 0 & -X \end{bmatrix} \begin{bmatrix} 1 \\ y_2 \\ y_1 \\ y_1 y_2 \end{bmatrix} .$$

The Reed-Muller form for this sequential circuit is given by

$$B^T(\underline{y}^+) = R(\underline{x})B^T(\underline{y}) \text{ over GF}(2)$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 \oplus x & 0 & x \\ 0 & 1 & 0 & 1 \oplus x \\ 0 & x & 0 & x \end{bmatrix} \begin{bmatrix} 1 \\ y_2 \\ y_1 \\ y_1 y_2 \end{bmatrix}$$

over GF(2) .