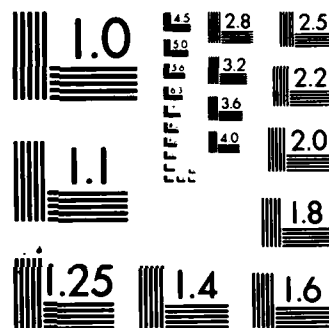


ON THE DISTRIBUTION OF COMPLEXITY FOR DE BRUIJN  
SEQUENCES(U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA  
R L HOLDAHL JUN 83

UNCLASSIFIED

F/G 12/1

NL



MICROCOPY RESOLUTION TEST CHART  
NATIONAL BUREAU OF STANDARDS 1963-A

2

# NAVAL POSTGRADUATE SCHOOL

Monterey, California

AD-A140 679



## THESIS

DTIC  
ELECTE  
MAY 2 1984  
S A D

ON THE DISTRIBUTION OF COMPLEXITY  
FOR DE BRUIJN SEQUENCES

Robert LaVern Holdahl

June 1983

Thesis Advisor:

H. Fredricksen

Approved for public release; distribution unlimited

DTIC FILE COPY

84 05 02 093

| REPORT DOCUMENTATION PAGE                                                                                                                                                                                                                                                                                                                                                                                                     |                                         | READ INSTRUCTIONS<br>BEFORE COMPLETING FORM                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|---------------------------------------------------------------------|
| 1. REPORT NUMBER                                                                                                                                                                                                                                                                                                                                                                                                              | 2. GOVT ACCESSION NO.<br><b>A140679</b> | 3. RECIPIENT'S CATALOG NUMBER                                       |
| 4. TITLE (and Subtitle)<br>On the Distribution of Complexity<br>for de Bruijn Sequences                                                                                                                                                                                                                                                                                                                                       |                                         | 5. TYPE OF REPORT & PERIOD COVERED<br>Master's Thesis;<br>June 1983 |
|                                                                                                                                                                                                                                                                                                                                                                                                                               |                                         | 6. PERFORMING ORG. REPORT NUMBER                                    |
| 7. AUTHOR(s)<br>Robert LaVern Holdahl                                                                                                                                                                                                                                                                                                                                                                                         |                                         | 8. CONTRACT OR GRANT NUMBER(s)                                      |
| 9. PERFORMING ORGANIZATION NAME AND ADDRESS<br>Naval Postgraduate School<br>Monterey, California 93940                                                                                                                                                                                                                                                                                                                        |                                         | 10. PROGRAM ELEMENT, PROJECT, TASK<br>AREA & WORK UNIT NUMBERS      |
| 11. CONTROLLING OFFICE NAME AND ADDRESS<br>Naval Postgraduate School<br>Monterey, California 93940                                                                                                                                                                                                                                                                                                                            |                                         | 12. REPORT DATE<br>June 1983                                        |
|                                                                                                                                                                                                                                                                                                                                                                                                                               |                                         | 13. NUMBER OF PAGES<br>71                                           |
| 14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)                                                                                                                                                                                                                                                                                                                                                   |                                         | 15. SECURITY CLASS. (of this report)                                |
|                                                                                                                                                                                                                                                                                                                                                                                                                               |                                         | 15a. DECLASSIFICATION/DOWNGRADING<br>SCHEDULE                       |
| 16. DISTRIBUTION STATEMENT (of this Report)<br><br>Approved for public release; distribution unlimited                                                                                                                                                                                                                                                                                                                        |                                         |                                                                     |
| 17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)                                                                                                                                                                                                                                                                                                                                    |                                         |                                                                     |
| 18. SUPPLEMENTARY NOTES                                                                                                                                                                                                                                                                                                                                                                                                       |                                         |                                                                     |
| 19. KEY WORDS (Continue on reverse side if necessary and identify by block number)<br><br>de Bruijn<br>complexity                                                                                                                                                                                                                                                                                                             |                                         |                                                                     |
| 20. ABSTRACT (Continue on reverse side if necessary and identify by block number)<br><br>Binary sequences have had application in communication systems for many years. Shift registers have been used in their generation, because of the ease and economy of their operation. For certain applications, nonlinear feedback functions are used by shift registers of span $n$ to generate sequences of lengths up to $2^n$ . |                                         |                                                                     |

## Block #20 Contd.

The sequences of maximum length  $2^n$  and their generation are the subject of this thesis. In particular the ways of generating these sequences using nonlinear feedback shift registers and their correlation to linear feedback shift registers are described. Complexity is the term given to the length of the shortest linear feedback shift register generating a maximum length  $2^n$  sequence.

Games and Chan [Ref. 1] have given considerable study to the subject of complexity. Some of the problems they left are discussed further in this paper. It will be shown that the complexity of a de Bruijn sequence (S) is the same as the complexity of its reverse ( $r S$ ), complement ( $\bar{S}$ ) and its reverse complement ( $r \bar{S}$ ). Sequences (S) for which  $r S = \bar{S}$  are termed RC sequences. It is shown that RC sequences exist for every odd  $n > 3$ . In addition a lower bound will be established for the number of RC sequences occurring for each odd  $n$ .



Approved for public release; distribution unlimited

On the Distribution of Complexity  
for de Bruijn Sequences

by

Robert LaVern Holdahl  
Major, United States Marine Corps  
B.S., South Dakota State University, 1972

Submitted in partial fulfillment of the  
requirements for the degree of

MASTER OF SCIENCE IN APPLIED MATHEMATICS

from the

NAVAL POSTGRADUATE SCHOOL  
June 1983

Author:

Robert L. Holdahl

Approved by:

Harold M. Friedman

Thesis Advisor

S. E. Latta

Chairman, Department of Mathematics

Kenneth T. Marshall

Dean of Information and Policy Sciences

## ABSTRACT

Binary sequences have had application in communication systems for many years. Shift registers have been used in their generation, because of the ease and economy of their operation. For certain applications, nonlinear feedback functions are used by shift registers of span  $n$  to generate sequences of lengths up to  $2^n$ .

The sequences of maximum length  $2^n$  and their generation are the subject of this thesis. In particular the ways of generating these sequences using nonlinear feedback shift registers and their correlation to linear feedback shift registers are described. Complexity is the term given to the length of the shortest linear feedback shift register generating a maximum length  $2^n$  sequence.

Games and Chan [Ref. 1] have given considerable study to the subject of complexity. Some of the problems they left are discussed further in this paper. It will be shown that the complexity of a de Bruijn sequence  $(S)$  is the same as the complexity of its reverse  $(r S)$ , complement  $(\bar{S})$ , and its reverse complement  $(r \bar{S})$ . Sequences  $(S)$  for which  $r S = \bar{S}$  are termed RC sequences. It is shown that RC sequences exist for every odd  $n \geq 3$ . In addition a lower bound will be established for the number of RC sequences occurring for each odd  $n$ .

## TABLE OF CONTENTS

|     |                                                                |    |
|-----|----------------------------------------------------------------|----|
| I.  | INTRODUCTION .....                                             | 11 |
| A.  | APPLICATION .....                                              | 11 |
| B.  | DEFINITION OF de BRUIJN SEQUENCES .....                        | 11 |
| C.  | PSEUDO-RANDOMNESS .....                                        | 12 |
| D.  | K-ARY SEQUENCES .....                                          | 13 |
| E.  | DEFINITIONS .....                                              | 13 |
| II. | SEQUENCE GENERATORS AND OPERATORS .....                        | 15 |
| A.  | SHIFT REGISTERS .....                                          | 15 |
| B.  | FEEDBACK SHIFT REGISTERS .....                                 | 15 |
| 1.  | Linear Feedback Functions .....                                | 16 |
| 2.  | Nonlinear Feedback Functions .....                             | 17 |
| 3.  | Comparison of Linear and Nonlinear<br>Feedback Functions ..... | 17 |
| C.  | SUCCESSOR AND PREDECESSOR STATES .....                         | 18 |
| D.  | de BRUIJN DIAGRAMS .....                                       | 20 |
| E.  | OPERATORS .....                                                | 22 |
| 1.  | Identity Operator .....                                        | 22 |
| 2.  | Reverse Operator .....                                         | 22 |
| 3.  | Complement Operator .....                                      | 22 |
| 4.  | Reverse Complement Operator .....                              | 24 |
| F.  | LINEAR RECURSION FORMULA .....                                 | 26 |
| 1.  | Pascal Triangle (Mod 2) .....                                  | 26 |
| 2.  | Pascal Triangle Properties .....                               | 27 |

|                                                                                  |    |
|----------------------------------------------------------------------------------|----|
| COMPLEXITY OF de BRUIJN SEQUENCES -----                                          | 28 |
| A. DEFINITION OF COMPLEXITY -----                                                | 28 |
| B. COMPLEXITY ALGORITHM -----                                                    | 28 |
| C. COMPLEXITY DISTRIBUTION -----                                                 | 30 |
| D. EFFECTS OF OPERATORS ON COMPLEXITY -----                                      | 30 |
| TRUTH TABLES -----                                                               | 35 |
| A. FULL TRUTH TABLE -----                                                        | 35 |
| B. HALF TRUTH TABLE -----                                                        | 36 |
| C. ZERO TRUTH TABLE -----                                                        | 37 |
| D. ONES TRUTH TABLE -----                                                        | 38 |
| E. EFFECTS OF CHANGING THE TRUTH TABLE -----                                     | 42 |
| F. SPECIAL NUMBERS -----                                                         | 48 |
| 1. Type RC Numbers -----                                                         | 49 |
| 2. Type R Numbers -----                                                          | 49 |
| G. GENERATOR ANALYSIS -----                                                      | 50 |
| RESULTS -----                                                                    | 56 |
| A. $\alpha(c, n) \equiv 0 \text{ MODULO } 4 \text{ FOR } n \text{ EVEN}$ -----   | 57 |
| B. RC SEQUENCES EXIST FOR ALL ODD $n \geq 3$ -----                               | 58 |
| C. LOWER BOUND ON NUMBER OF RC SEQUENCES -----                                   | 60 |
| 1. Theorem -----                                                                 | 60 |
| 2. Example for $n = 7$ -----                                                     | 60 |
| CONJECTURES -----                                                                | 63 |
| A. RC SEQUENCE GENERATOR TECHNIQUE -----                                         | 63 |
| B. PROBLEMS -----                                                                | 65 |
| APPENDIX A: ALGORITHM FOR GENERATING LEAST<br>ELEMENT FOR EVERY PURE CYCLE ----- | 67 |

|                                 |    |
|---------------------------------|----|
| LIST OF REFERENCES -----        | 70 |
| INITIAL DISTRIBUTION LIST ----- | 71 |

## LIST OF TABLES

|      |                                                                              |    |
|------|------------------------------------------------------------------------------|----|
| 1.1  | 3-TUPLE COMPOSITION OF de BRUIJN<br>SEQUENCES OF SPAN 3 -----                | 12 |
| 2.1  | ADDITION (MODULO 2) -----                                                    | 17 |
| 2.2  | MULTIPLICATION (MODULO 2) -----                                              | 17 |
| 2.3  | NUMBER OF MAXIMUM LENGTH SEQUENCES -----                                     | 19 |
| 2.4  | CONJUGATE AND COMPANION STATES (n=3) -----                                   | 20 |
| 2.5  | de BRUIJN SEQUENCE OPERATORS -----                                           | 25 |
| 2.6  | PASCAL TRIANGLE (MOD 2) -----                                                | 26 |
| 3.1  | LIMITS OF COMPLEXITY -----                                                   | 29 |
| 3.2  | COMPLEXITY DISTRIBUTION -----                                                | 32 |
| 4.1  | FULL TRUTH TABLE OF (00011101) -----                                         | 36 |
| 4.2  | HALF TRUTH TABLE OF (00011101) -----                                         | 37 |
| 4.3  | ZERO TRUTH TABLE FOR n = 3 -----                                             | 38 |
| 4.4  | ONES TRUTH TABLE (n = 3) -----                                               | 40 |
| 4.5  | PURE CYCLE COMPILATION -----                                                 | 41 |
| 4.6  | TRUTH TABLE (TABLE 4.4 MODIFIED) -----                                       | 43 |
| 4.7  | TRUTH TABLE (TABLE 4.6 MODIFIED) -----                                       | 43 |
| 4.8  | TRUTH TABLE ANALYSIS CHART -----                                             | 51 |
| 4.9  | GENERATOR ANALYSIS FOR de BRUIJN<br>SEQUENCES ( $r \ S \neq \bar{S}$ ) ----- | 52 |
| 4.10 | FULL TRUTH TABLE FOR S -----                                                 | 53 |
| 4.11 | FULL TRUTH TABLE FOR $\bar{S}$ (NON STANDARD) -----                          | 54 |
| 4.12 | FULL TRUTH TABLE FOR $\bar{S}$ -----                                         | 55 |
| 5.1  | PURE CYCLES FOR N=7 & wt $\leq$ 3 -----                                      | 61 |

|     |                                                             |    |
|-----|-------------------------------------------------------------|----|
| 5.2 | ADJACENCY MATRIX FOR $n=7$ -----                            | 62 |
| 6.1 | RC GENERATOR TECHNIQUE -----                                | 64 |
| 6.2 | RC de BRUIJN SEQUENCE 0 (Mod 4)<br>GROUPING FOR $n=5$ ----- | 66 |
| A.1 | $\Omega$ ALGORITHM FOR $N = 7$ -----                        | 68 |
| A.2 | PURE CYCLE LEAST ELEMENTS ( $n=7$ ) -----                   | 69 |

## LIST OF FIGURES

|     |                                          |    |
|-----|------------------------------------------|----|
| 2.1 | n-Stage Shift Register -----             | 15 |
| 2.2 | n-Stage Feedback Shift Register -----    | 16 |
| 2.3 | Adjacency Quadruple -----                | 20 |
| 2.4 | Graph $G_3$ -----                        | 21 |
| 2.5 | A Hamiltonian Path through $G_3$ -----   | 23 |
| 3.1 | Flowchart for Complexity Algorithm ----- | 31 |
| 4.1 | Pure Cycles ( $n=3$ ) -----              | 39 |
| 4.2 | Complementing Cycles ( $n=3$ ) -----     | 42 |
| 4.3 | Cyclic Composition of Table 4.4 -----    | 44 |
| 4.4 | Cyclic Composition of Table 4.7 -----    | 45 |
| 4.5 | Two Cycle Graph -----                    | 46 |
| 4.6 | Cycle Splitting -----                    | 47 |
| 4.7 | Cycle Joining -----                      | 48 |

## I. INTRODUCTION

### A. APPLICATION

de Bruijn sequences have been the subject of recurring interest since their discovery over a century ago. Recent developments in radar ranging [Ref. 2: Ch. 13], error correcting codes, secure or limited access code generators [Ref. 3: pp. 12-14], and mathematical modeling have made application of de Bruijn sequences because of their properties. The binary shift registers readily model digital computers with electronic states where "1" indicates the on state and "0" indicates the off state.

### B. DEFINITION OF de BRUIJN SEQUENCES

For a positive integer  $n$ , a de Bruijn sequence of span  $n$  is a complete binary cycle of length  $2^n$  which is a sequence  $S = \{s_1, s_2, \dots, s_{2^n}\}$  taken in circular order ( $s_1$  follows  $s_{2^n}$ ) such that all possible  $n$ -tuples occur exactly once. [Ref. 4: p. 120]. Complete binary cycles are often called de Bruijn sequences after the Dutch mathematician, N. de Bruijn, who in 1946 proved the existence of complete binary cycles having length  $2^n$  and that they numbered  $2^{2^{n-1}-n}$ . de Bruijn was preceded by Flye Saint-Marie a half century earlier in an obscure publication [Ref. 5]. As an example for  $n = 3$ , Table 1.1 shows both  $(2^{2^{3-1}-3})$  de Bruijn sequences

of length eight ( $2^3$ ). Both of these sequences are examined to confirm that each of the eight 3-tuples occur exactly once. Notice that 2 elements of the sequence are repeated as signified by the bar ( $\overline{00}$ ), which was necessary on each sequence to complete the last two 3-tuples.

TABLE 1.1  
3-TUPLE COMPOSITION OF de BRUIJN SEQUENCES OF SPAN 3

|                          |                          |
|--------------------------|--------------------------|
| 00011101 $\overline{00}$ | 00010111 $\overline{00}$ |
| 000                      | 000                      |
| 001                      | 001                      |
| 011                      | 010                      |
| 111                      | 101                      |
| 110                      | 011                      |
| 101                      | 111                      |
| 010                      | 110                      |
| 100                      | 100                      |

There are  $2^n$  different possible starting points for each de Bruijn sequence; however, each cyclic permutation is considered equivalent. It is often a matter of convenience to start each sequence in a canonical way with the all zero or all one  $n$ -tuple. This reduces confusion when working with a number of different de Bruijn sequences.

### C. PSEUDO-RANDOMNESS

Since each binary  $n$ -tuple occurs exactly once on the cycle, the sequence models a uniform distribution with the probability of given  $n$ -tuple occurring to be exactly  $1/2^n$ . The sequence is not entirely random, however, since each

$n$ -tuple  $(a_1 a_2 \cdots a_n)$  has but two possible successors  $(0 a_1 a_2 \cdots a_{n-1}$  or  $1 a_1 a_2 \cdots a_{n-1})$ . de Bruijn sequences satisfy the randomness properties of equidistribution of 0's and 1's and run lengths [Ref. 3: p. 10] which would be expected from the tossing of a fair coin. Thus, de Bruijn sequences have a pseudorandom property.

#### D. K-ARY SEQUENCES

In general it is possible to work with  $k$  possible states for each position of an  $n$ -tuple. Flye Saint-Marie in 1894, showed the existence and determined the number of complete cycles for  $n$ -tuples of  $k$  characters to be  $[(k-1)!]^{k^{n-1}} k^{k^{n-1}-n}$ . [Ref. 5]. This report is restricted to the binary case ( $k = 2$ ) due to its principal application in electronic communications and computers.

#### E. DEFINITIONS

For  $S = \{s_1 s_2 \cdots s_k\}$  where  $s_i \in \{0,1\}$  for  $1 \leq i \leq k$  the following are defined:

1. Let  $W(S)$  denote the weight of  $S$ .

$$W(S) = \sum_{i=1}^k s_i$$

2. Let  $P(S)$  denote the parity of  $S$ .

$$P(S) = \sum_{i=1}^k s_i \pmod{2}$$

3. Let  $l(S)$  denote the length of  $S$ .

$l(s) = k$  where  $k$  is the number of positions in  $S$ .

## II. SEQUENCE GENERATORS AND OPERATORS

### A. SHIFT REGISTERS

In practice shift registers are used to generate de Bruijn sequences. An  $n$ -stage shift register has  $n$  memory registers ( $x_1, x_2, \dots, x_n$ ) which shift their contents (0 or 1) to the next register upon command. For example, in Fig. 2.1, the contents of  $x_1$  will transfer to  $x_2$ ,  $x_2$  to  $x_3$ , etc., at the appropriate time with  $x_n$  serving as the output. However, the contents of an  $n$ -stage shift register would empty in  $n$  shifts if no input was provided to  $x_1$ .



Fig. 2.1  $n$ -Stage Shift Register.

### B. FEEDBACK SHIFT REGISTERS

Feedback networks are added to provide an input to the 1st stage of the shift register. Note that in practice the output can be taken from any stage of the shift register. In fact, the contents of any stage is the same as the contents of any stage is the same as the contents of the  $n^{\text{th}}$

stage, merely shifted by a certain amount. In Fig. 2.2 the feedback function  $f$  is added to the  $n$ -stage shift register to generate non-trivial sequences. The coefficients  $a_0, a_1, \dots, a_n$  are 0 or 1 with  $a_0 = a_n = 1$ .

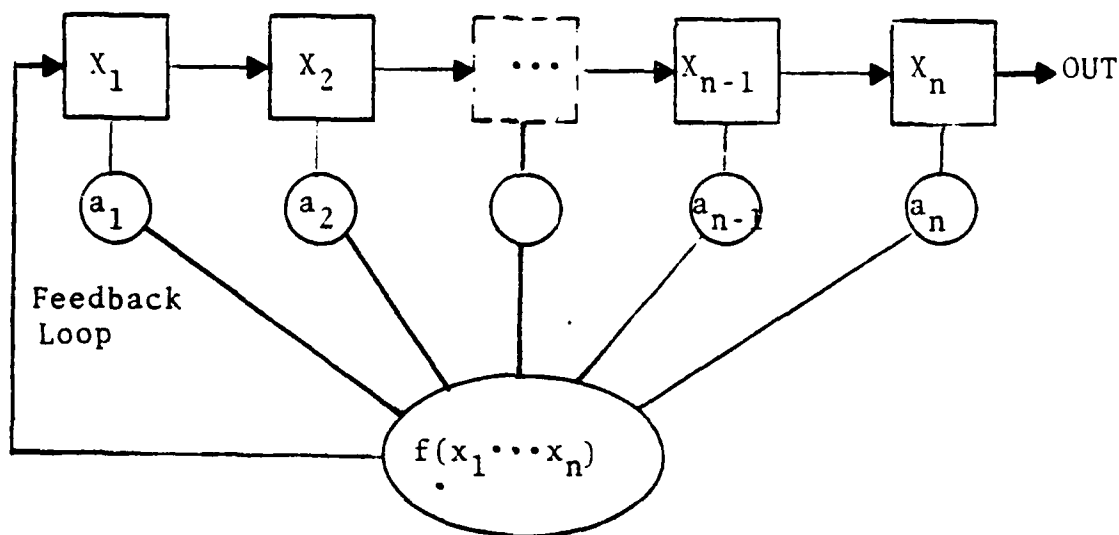


Fig. 2.2  $n$ -Stage Feedback Shift Register.

### 1. Linear Feedback Functions

A feedback function  $f$  is classified as linear if the function  $f(x_1, x_2, \dots, x_n)$  is restricted to be of the form  $f = \sum_{i=1}^n a_i x_i$  where the addition is modulo 2 addition. The addition (mod 2) table is given in Table 2.1 below. Note that subtraction is equivalent to addition when operating modulo 2.

TABLE 2.1  
ADDITION (MODULO 2)

| $\oplus$ | 0 | 1 |
|----------|---|---|
| 0        | 0 | 1 |
| 1        | 1 | 0 |

## 2. Nonlinear Feedback Functions

If the feedback function  $f(x_1, \dots, x_n)$  utilizes multiplication (mod 2) and addition (mod 2) then the feedback function is nonlinear. (We also say that the linear feedback functions are vacuously nonlinear feedback functions.) Modulo 2 multiplication is identical to multiplication in the integers with the restriction of the alphabet used being the set  $\{0, 1\}$  as described in Table 2.2.

TABLE 2.2  
MULTIPLICATION (MODULO 2)

| $\cdot$ | 0 | 1 |
|---------|---|---|
| 0       | 0 | 0 |
| 1       | 0 | 1 |

## 3. Comparison of Linear and Nonlinear Feedback Functions

Considerable research has been devoted to the study of linear feedback functions because of their ease of analysis. Nonlinear feedback functions are much more complicated.

However, the class of sequences that can be generated by nonlinear functions is much greater than for linear functions.

The number of binary maximum length  $(2^n - 1)$  linear sequences that can be generated by a  $n$ -stage linear feedback shift register (LFSR) is approximately  $\frac{2^n}{n}$  [Ref. 7]. The reason that the maximum length linear sequences only have length  $2^n - 1$  is that the zero state is a fixed point under the linear function. This poses no problem since the maximal length linear sequences are readily made into de Bruijn sequences having length  $2^n$  simply by adding a zero to the  $(n-1)$ -tuple of zeros. The feedback function involved then becomes a nonlinear function.

By comparison the number of binary nonlinear full length sequences  $(2^n)$  that can be generated by a nonlinear feedback shift register (NFSR) is exactly  $2^{2^{n-1} - n}$ . Below, Table 2.3 compares these numbers for  $3 \leq n \leq 8$ . The number of maximum length sequences will be of interest later in Section III, where the concept of complexity in generating these sequences will be developed. Various algorithms are listed in a survey by Fredricksen [Ref. 5] for generating de Bruijn sequences.

### C. SUCCESSOR AND PREDECESSOR STATES

The contents of an  $n$ -stage shift register at a specific time is usually referred to as its "state". As mentioned in Section I when discussing the pseudorandomness of de Bruijn

TABLE 2.3  
NUMBER OF MAXIMUM LENGTH SEQUENCES

| <u>n</u> | <u>Linear</u> | <u>Nonlinear</u>     |
|----------|---------------|----------------------|
| 3        | 2             | 2                    |
| 4        | 4             | 16                   |
| 5        | 6             | 2048                 |
| 6        | 6             | 67,108,864           |
| 7        | 18            | $1.4 \times 10^{17}$ |
| 8        | 30            | $2.7 \times 10^{36}$ |

sequences each state has two possible successor (conjugate) states depending on whether the feedback function generates a "0" or "1" as the input to register  $x_1$ . Likewise each state has two predecessor (companion) states depending on whether the previous output was a "0" or "1". The adjacency quadruple in Fig. 2.3 centers around then  $(n-1)$ -tuple  $x_2 \cdots x_n$ . That is, each input state has two possible successors depending on whether the feedback is 0 or 1, and each output state has two possible predecessors depending on whether the previous output from the  $n^{\text{th}}$  stage was 0 or 1.

In Table 2.4 we show an example for  $n = 3$  of the possible successors and predecessors for each state.

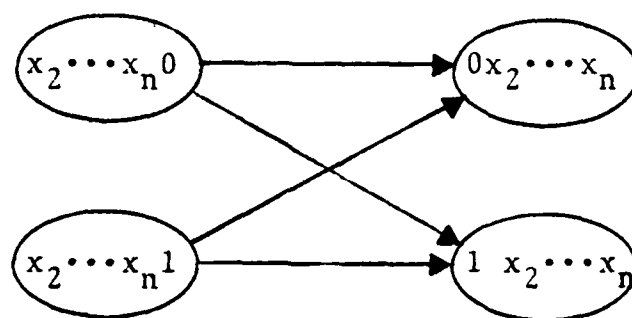


Fig. 2.3 Adjacency Quadruple.

TABLE 2.4

CONJUGATE AND COMPANION STATES ( $n=3$ )

| <u>Predecessors</u>                                                                       | <u>State</u> | <u>Successors</u>                                                                        |
|-------------------------------------------------------------------------------------------|--------------|------------------------------------------------------------------------------------------|
| 000-001                                                                                   | 000          | 000-100                                                                                  |
| 010-011                                                                                   | 001          | 000-100                                                                                  |
| 100-101                                                                                   | 010          | 001-101                                                                                  |
| 110-111                                                                                   | 011          | 001-101                                                                                  |
| 000-001                                                                                   | 100          | 010-110                                                                                  |
| 010-011                                                                                   | 101          | 010-110                                                                                  |
| 100-101                                                                                   | 110          | 011-111                                                                                  |
| 110-111                                                                                   | 111          | 011-111                                                                                  |
| <div style="text-align: center;"> <math>\uparrow \quad \uparrow</math><br/> Output </div> |              | <div style="text-align: center;"> <math>\uparrow \quad \uparrow</math><br/> Input </div> |

#### D. de BRUIJN DIAGRAMS

The de Bruijn diagram compactly contains all the above information. The diagram contains  $2^n$  vertices corresponding to the  $2^n$  states and two directed edges from each state to

the possible pair of successor vertices. As a result two arrows exit every vertex leading to conjugate states, and two arrows enter every vertex arriving from companion states. For an example consider the de Bruijn diagram  $G_n$  for  $n = 3$  in Fig. 2.4. An Eulerian path through  $G_n$  is defined as a

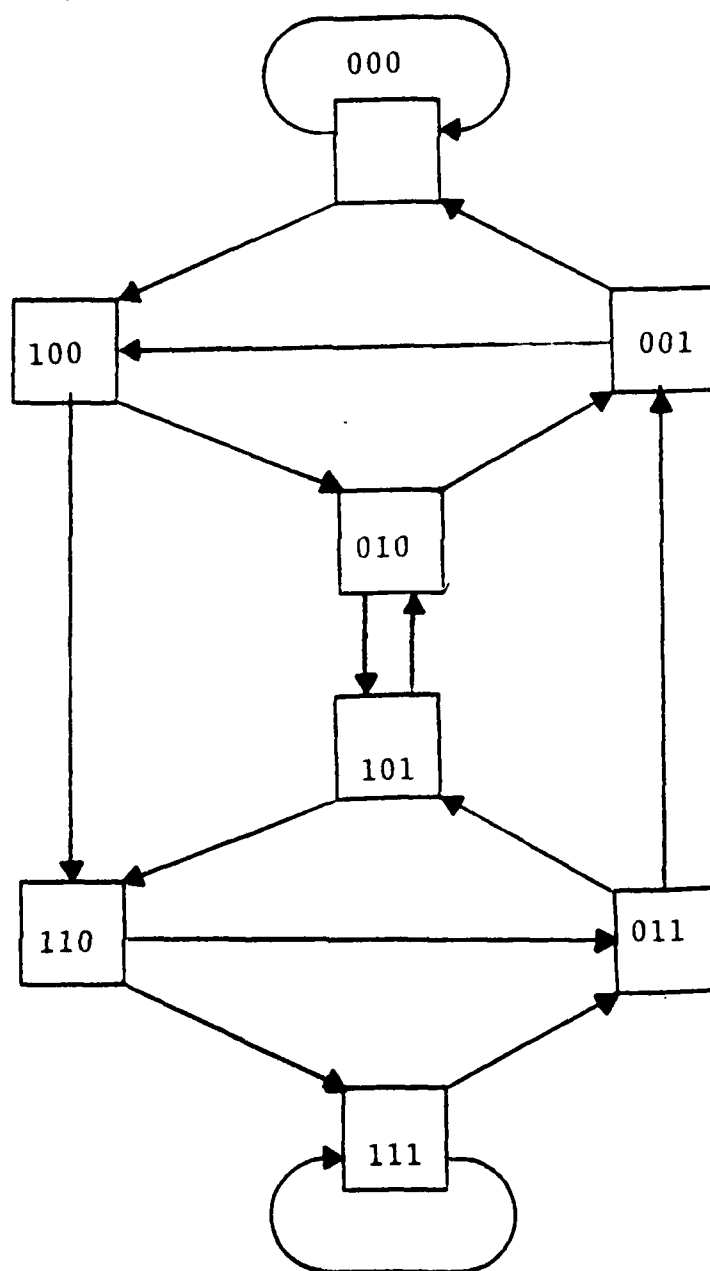


Fig. 2.4 Graph  $G_3$ .

path which visits each edge exactly once. A path which visits every vertex of  $G_n$  is called a Hamiltonian path. A Hamiltonian path in  $G_n$  is a de Bruijn sequence of span  $n$ . If the edges of  $G_n$  are labeled with an  $n + 1$ -tuple defined by the labels on the predecessor and successor states, then the Eulerian paths in  $G_n$  correspond to Hamiltonian paths-- and de Bruijn sequences in the graph  $G_{n+1}$ . The Hamiltonian path in Fig. 2.5 is a subgraph of  $G_3$  in Fig. 2.4 with exactly one edge emanating from each vertex.

#### E. OPERATORS

For  $S = s_1 s_2 \cdots s_{n-1} s_n$  where  $s_i \in \{0,1\}$  for  $1 \leq i \leq n$  the following operators are defined.

##### 1. Identity Operator

The identity operator ( $e$ ) operating on  $S$  denoted

$$eS = s_1 s_2 \cdots s_{n-1} s_n = S.$$

##### 2. Reverse Operator

The reverse operator ( $r$ ) operating on  $S$  is denoted  $r S$ , where  $r S = s_n s_{n-1} \cdots s_2 s_1$ . The reverse operator preserves the weight, parity and length of  $S$ . Note also that  $(r)^2 \equiv e$ .

##### 3. Complement Operator

The complement (dual) operator on  $S$  is denoted  $d S$  or  $\bar{S}$ , where  $\bar{S} = \bar{s}_1 \bar{s}_2 \cdots \bar{s}_{n-1} \bar{s}_n$  such that  $\bar{s}_i = s_i \oplus 1 \pmod{2}$  for  $1 \leq i \leq n$ .

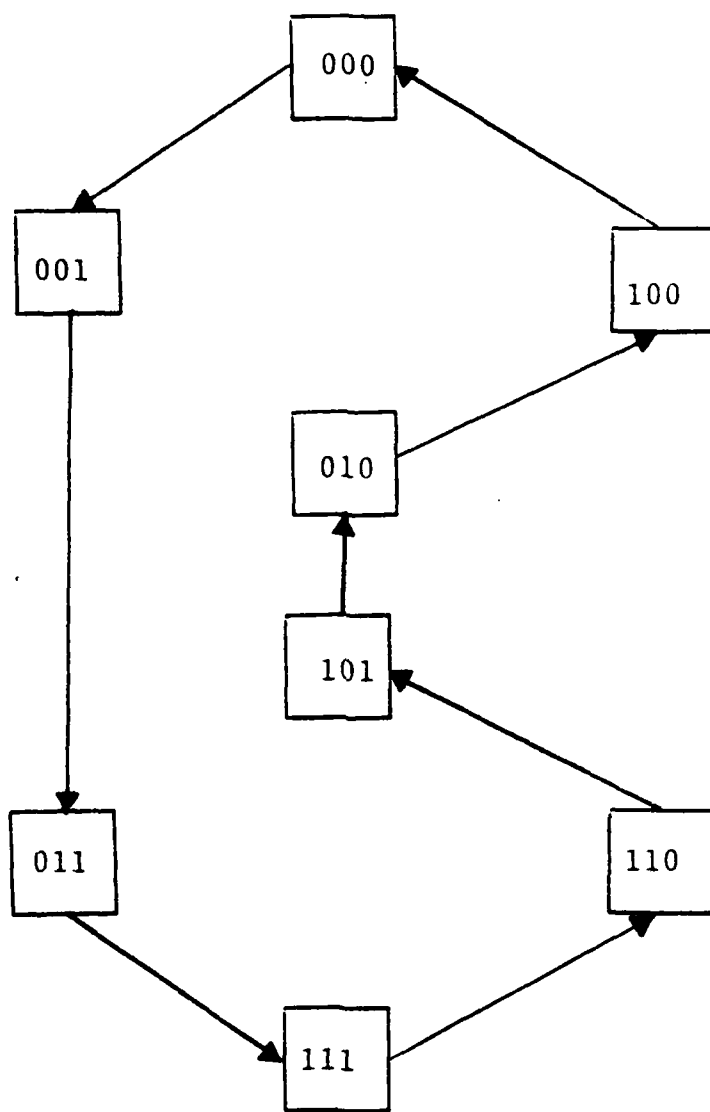


Fig. 2.5 A Hamiltonian Path through  $G_3$ .

Lemma 1: If  $W(S) = k$  for  $S = s_1 s_2 \cdots s_n$  then  
 $W(\bar{S}) = n-k$ .

Proof:  $W(S) = k$  implies  $k$  nonzero elements  $\in S$   
 and  $n-k$  zero elements  $\in S$ .

Complementing  $n-k$  zero elements produces  
 $n-k$  nonzero elements  $\in \bar{S}$ .

$\therefore W(\bar{S}) = n-k$

Q.E.D.

Lemma 2: If  $P(S) = a$  where  $a \in \{0,1\}$  and  $S = \{s_1 s_2 \cdots s_n\}$ ,  
 then  $P(\bar{S})$  is  $a$  iff  $n$  is even.

Proof:  $P(S) = \sum_{i=1}^n s_i \pmod{2} = a$

$$P(\bar{S}) = \sum_{i=1}^n \bar{s}_i \pmod{2} = \sum_{i=1}^n s_i \oplus 1 = a \oplus n$$

therefore  $P(\bar{S}) = P(n-a)$

Q.E.D.

Also note  $(d)^2 = e$ , and that the reverse and complement operators are commutative, i.e.  $rd = dr$ .

#### 4. Reverse Complement Operator

The reverse complement operator on  $S$  is denoted  
 $r\bar{S} = \bar{s}_n \bar{s}_{n-1} \cdots \bar{s}_2 \bar{s}_1$ . Weight and parity are effected  
 by the reverse complement operator exactly as with the  
 complementation operator.

These operators apply to sequences as well, since  
 sequences are composed of  $n$ -tuples. Table 2.6 shows the  
 effect of operators on de Bruijn sequences of span 3 and 4

where  $rS$ ,  $\bar{S}$ , and  $r\bar{S}$  are all de Bruijn sequences, as they always are if  $S$  is a de Bruijn sequence.

TABLE 2.5  
de BRUIJN SEQUENCE OPERATORS

| <u>n = 3</u>          | (Canonical Form) |
|-----------------------|------------------|
| $S = 00011101$        | $= 00011101$     |
| $rS = 10111000$       | $= 00010111$     |
| $\bar{S} = 11100010$  | $= 00010111$     |
| $r\bar{S} = 01000111$ | $= 00011101$     |

| <u>n = 4</u>                  | (Canonical Form)     |
|-------------------------------|----------------------|
| $S = 0000111101001011$        | $= 0000111101001011$ |
| $rS = 1101001011110000$       | $= 0000110100101111$ |
| $\bar{S} = 1111000010110100$  | $= 0000101101001111$ |
| $r\bar{S} = 0010110100001111$ | $= 0000111100101101$ |

If as in the case for  $n = 3$  in Table 2.5 a sequence  $S$  is equivalent to its reverse complement, then  $S$  is termed a RC sequence. This applies to both de Bruijn and non-de Bruijn sequences. The following theorem appears in a paper by Etzion and Lempel [Ref. 6].

Theorem 1: A sequence  $S$  is a RC sequence if  $\ell(S)$  is even and  $S = \{X, r\bar{X}\}$  for some  $X$  where  $X$  is a binary string.

## F. LINEAR RECURSION FORMULA

de Bruijn sequences generated by a nonlinear function can also be generated by a linear function  $f(x_1 \cdots x_n) = x_0$  having the linear recursion formula

$$\sum_{j=0}^n a_j x_j = 0.$$

Here each  $a_j$  determines a tap to the  $j^{\text{th}}$  stage of the register. The linear generator polynomial must be  $(x + 1)^k$  for some positive integer  $k$ , due to the periods of de Bruijn sequences  $(2^n)$  and results from theorems given by Golomb [Ref. 7: pp. 27-43].

### 1. Pascal Triangle (Mod 2)

The values for each  $a_j$  are summarized in the Pascal triangle (mod 2) Table 2.6 for various values of  $n$ . They are the coefficients generated by the binomial expansion of  $(x + 1)^k \text{ mod } 2$ .

TABLE 2.6  
PASCAL TRIANGLE (MOD 2)

|       |       |       |       |       |       |       |   |           |
|-------|-------|-------|-------|-------|-------|-------|---|-----------|
| k = 0 |       |       |       |       |       |       | 1 |           |
| 1     |       |       |       |       |       | 1     | 1 |           |
| 2     |       |       |       |       | 1     | 0     | 1 |           |
| 3     |       |       |       | 1     | 1     | 1     | 1 |           |
| 4     |       |       | 1     | 0     | 0     | 0     | 0 | 1         |
| 5     |       | 1     | 1     | 0     | 0     | 1     | 1 |           |
|       | $a_0$ | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ |   | $(x+1)^5$ |

## 2. Pascal Triangle Properties

(a) The  $a_j$  sequence is palindromic, that is

$$a_0 = a_n = 1, a_1 = a_{n-1}, a_2 = a_{n-2}, \text{ etc.}$$

(b) The number of nonzero coefficients is even,

that is  $\sum_{j=0}^n a_j = 0 \pmod{2}.$

### III. COMPLEXITY OF de BRUIJN SEQUENCES

#### A. DEFINITION OF COMPLEXITY

The term complexity indicates a general measure of the predictability of a sequence. Various definitions of complexity are in use, but this paper will use the one given by Chan and Games [Ref. 1]. Their definition of complexity is the length of the shortest LFSR required to generate a sequence. They apply their results primarily to de Bruijn sequences. This definition is also the one used by Herlestom [Ref. 8] to look at two different shift register cycle generators. For a de Bruijn sequence  $S$ , let  $C(S)$  denote the complexity of  $S$ .

Previous results by Chan and Games [Ref. 1] establish lower and upper bounds of  $2^{n-1}+n$  and  $2^{n-1}$  respectively for the complexity of a de Bruijn sequence. Thus, the length of a LFSR is almost as long the sequence as opposed to a  $n$ -stage NFSR which generates the sequence. Table 3.1 serves as a ready reference for the upper and lower limits of complexity for  $3 \leq n \leq 8$ . The upper bound is known to be attained for all  $n$  and the lower bound for all  $n \leq 6$ .

#### B. COMPLEXITY ALGORITHM

A fast method for determining the complexity of a de Bruijn sequence was developed by Games and Chan [Ref. 9]

TABLE 3.1  
LIMITS OF COMPLEXITY

| Span<br>(n) | Lower Bound<br>$(2^{n-1} + n)$ | Upper Bound<br>$= (2^n - 1)$ |
|-------------|--------------------------------|------------------------------|
| 3           | 7                              | 7                            |
| 4           | 12                             | 15                           |
| 5           | 21                             | 31                           |
| 6           | 38                             | 63                           |
| 7           | 71                             | 127                          |
| 8           | 136                            | 255                          |

and is represented by the flow chart in Fig. 3.1. Let  $S$  be a de Bruijn sequence then  $\ell(S) = 2^n$ . Further let  $S = A:B = D$  where  $A = \{a_1 a_2 \dots a_{2^{n-1}}\}$  and  $B = \{b_1 b_2 \dots b_{2^{n-1}}\}$  then  $D = \{a_1 a_2 \dots a_{2^{n-1}} b_1 b_2 \dots b_{2^{n-1}}\}$ . To serve as a guide an example for  $n = 5$  is now presented. Let the de Bruijn sequence  $S = \{11111000001000110101100101001110\}$  having length  $\ell = 32$ .

|     |                         |               |
|-----|-------------------------|---------------|
| A   | 1111100000100011        | $\ell = 16$   |
| B   | <u>0101100101001110</u> | <u>C = 0</u>  |
| A+B | 1010000101101101        | C = 16        |
| A   | 10100001                | $\ell = 8$    |
| B   | <u>01101101</u>         | <u>C = 16</u> |
| A+B | 11001100                | C = 24        |

|          |             |                            |                        |
|----------|-------------|----------------------------|------------------------|
| A        | 1100        | $\ell = 4$                 | Since $A \oplus B = 0$ |
| <u>B</u> | <u>1100</u> | <u><math>C = 24</math></u> |                        |
| A+B      | 0000        | $C = 24$                   | C is unchanged         |
|          |             |                            |                        |
| A        | 11          | $\ell = 2$                 |                        |
| <u>B</u> | <u>00</u>   | <u><math>C = 24</math></u> |                        |
| A+B      | 11          | $C = 26$                   |                        |
|          |             |                            |                        |
| A        | 1           | $\ell = 1$                 | Add 1 since $\ell = 1$ |
| <u>B</u> | <u>1</u>    | <u><math>C = 26</math></u> | & $A = 1$              |
| A+B      | 0           | $C = 26$                   | + 1 = 27               |

#### C. COMPLEXITY DISTRIBUTION

The nature of the distribution of complexity of de Bruijn sequences is the primary interest of this paper. Let  $\alpha(c, n)$  denote the number of de Bruijn sequences having complexity  $c$  and span  $n$ . The complexity distribution of de Bruijn sequences of span  $n$  for  $3 \leq n \leq 6$  are listed in Table 3.2. Unfortunately the large number of de Bruijn sequences for  $n \geq 7$  ( $2^{57}$ ) does not allow an exhaustive examination of their complexities.

Examination of this data led Chan and Games to conjecture that for  $n \geq 3$   $\alpha(c, n)$  is congruent to 0 modulo 4.

#### D. EFFECTS OF OPERATORS ON COMPLEXITY

Chan et al. [Ref. 1] proved that  $\alpha(c, n)$  for  $n \geq 3$  was congruent to 0 modulo 2. By showing that for each de Bruijn

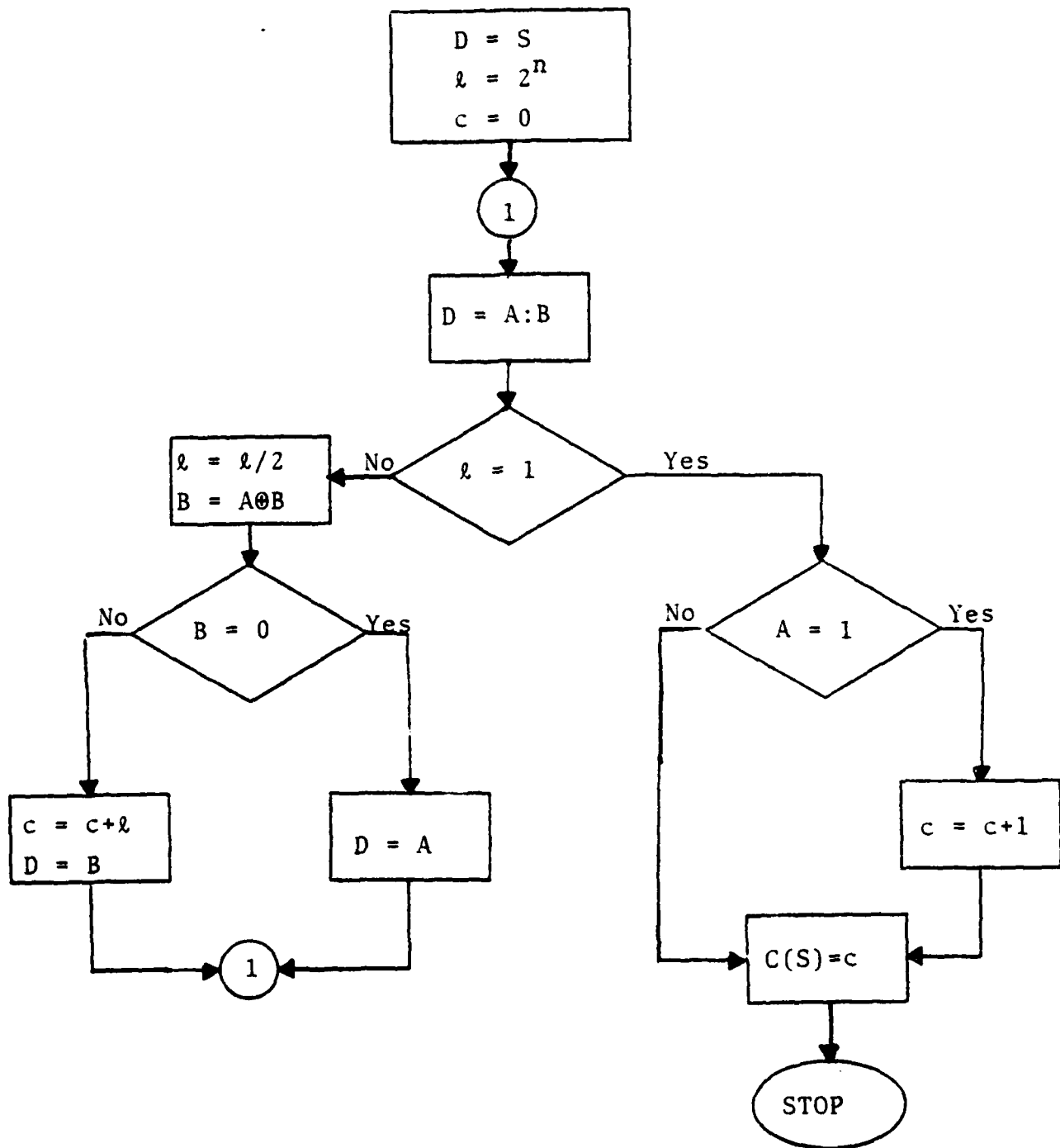


Fig. 3.1 Flowchart for Complexity Algorithm.

TABLE 3.2  
COMPLEXITY DISTRIBUTION

| n = 4 |                | n = 5 |                |    |                |
|-------|----------------|-------|----------------|----|----------------|
| c     | $\alpha(c, 4)$ | c     | $\alpha(c, 5)$ | c  | $\alpha(c, 5)$ |
| 12    | 4              | 21    | 8              | 27 | 64             |
| 13    | 0              | 22    | 0              | 28 | 180            |
| 14    | 4              | 23    | 12             | 29 | 224            |
| 15    | 8              | 24    | 20             | 30 | 448            |
|       |                | 25    | 32             | 31 | 1024           |
|       |                | 26    | 36             |    |                |

| n = 6 |                |    |                |
|-------|----------------|----|----------------|
| c     | $\alpha(c, 6)$ | c  | $\alpha(c, 6)$ |
| 38    | 448            | 51 | 8704           |
| 39    | 0              | 52 | 18096          |
| 40    | 32             | 53 | 34224          |
| 41    | 96             | 54 | 67700          |
| 42    | 160            | 55 | 126592         |
| 43    | 80             | 56 | 259320         |
| 44    | 432            | 57 | 519752         |
| 45    | 288            | 58 | 1041252        |
| 46    | 896            | 59 | 2090716        |
| 47    | 1168           | 60 | 4162352        |
| 48    | 2772           | 61 | 8342176        |
| 49    | 2352           | 62 | 16692832       |
| 50    | 5224           | 63 | 33731200       |

sequence having complexity  $c$ , there exists another different de Bruijn sequence  $\bar{S}$  also having complexity  $c$ . Consequently they showed that the complement operator does not change the complexity of a de Bruijn sequence. Using a different approach, the next theorem will show that the complexity of a de Bruijn sequence is also the complexity of the de Bruijn sequences defined by the reverse operator and by the reverse complement operator as well.

Lemma 3. For  $S = \{s_1 s_2 \cdots s_{2^n-1}\}$ , a de Bruijn sequence,  $C(S) = c$  iff  $\sum_{i=0}^c a_i s_i = 0$  for every  $s_i$  where each  $a_i$  comes from the  $c^{\text{th}}$  row of the Pascal triangle (mod 2) and  $c$  is the smallest integer such that the above recursion holds.

Proof.  $S$  is de Bruijn with  $C(S) = c$  iff  $s_i = f(s_{i+1} \cdots s_{i+c})$  for every  $s_i \in S$ , which is equivalent to  $s_i = \sum_{j=1}^c a_j s_{i+j}$  from results by Golomb [Ref. 5: pp. 27-43] mentioned earlier. In turn  $s_i = \sum_{j=0}^c a_j s_{i+j} = 0$  from properties of the Pascal triangle given in Section II. Q.E.D.

This lemma is used in the following theorem to show that complexity is preserved by various operators on de Bruijn sequences.

Theorem 2. If  $S$  is a de Bruijn sequence having complexity  $C$ , then  $C(S) = C(\bar{S}) = C(rS) = C(r\bar{S}) = c$ .

Proof. Part I (reverse operator)

Let  $s_i s_{i+1} \cdots s_{i+c}$  be an arbitrary  $(c+1)$  long segment of  $S$  which satisfies

$$(1) \sum_{j=0}^c a_j s_{i+j} = 0$$

by Lemma 3. Since the  $a_j$  sequence is palindromic as shown earlier,  $s_{i+c} \cdots s_{i+1} s_i$  a  $(c+1)$  long segment of  $rS$  satisfies equation (1). Thus  $C(rS) = c$ .

Part II (complement operator) substituting  $\bar{s}_i \cdots \bar{s}_{i+c}$ , the  $c+1$  long segment of  $\bar{S}$ , into equation (1), the results are  $a_0 \bar{s}_i + a_1 \bar{s}_{i+1} + \cdots + a_{c-1} \bar{s}_{i+c-1} + a_c \bar{s}_{i+c} =$

$$a_0 (s_i + 1) + a_1 (s_{i+1} + 1) + \cdots + a_{c-1} (s_{i+c-1} + 1) + a_c$$

$$(s_{i+c} + 1) = \sum_{j=0}^c a_j s_{i+j} + \sum_{j=0}^c a_j \pmod{2}. \text{ Since there are}$$

an even number of nonzero  $a_j$ 's,  $\sum_{j=0}^c a_j = 0$  and equation (1) is satisfied. Therefore, by Lemma 3  $C(\bar{S}) = c$ .

Part III (reverse complement operator), by Parts I and II, it follows immediately that  $C(r\bar{S}) = c$ . Thus  $C(S) = C(rS) - C(\bar{S}) = C(r\bar{S})$

Q.E.D.

#### IV. TRUTH TABLES

Linear and nonlinear feedback functions were used in conjunction with n-stage shift registers to generate de Bruijn sequences in Section II. The input  $x_0$  was generated as some function  $f$  of the current state  $x_1 x_2 \dots x_n$ , that is

$$(1) \quad x_0 = f(x_1 x_2 \dots x_n)$$

or equivalently writing  $f$  as in (2) when specializing for cycles only functions.

$$(2) \quad x_0 = x_n + g(x_1 \dots x_{n-1}).$$

Extensive use is made of equation (2) since results for cycles only are desired.

##### A. FULL TRUTH TABLE

The full truth table is a useful way of listing the functional value  $x_0$  from equation (1) for each possible state of the shift register. The functional values in Table 4.1 is an example of a full truth table for a de Bruijn sequence (00011101).

Examining the full truth table it becomes apparent that the information in the lower half (below the dashed line) is redundant, since the values of  $f(x_1 x_2 x_3)$  for  $x_3 = 1$  in the lower half are merely the complements of the values of  $f(x_1 x_2 x_3)$  for  $x_3 = 0$  in the upper half for the identical values of  $x_1 x_2$ . This suggests that the upper half (or the

TABLE 4.1  
FULL TRUTH TABLE OF (00011101)

| Current State<br>( $x_3 \ x_2 \ x_1$ ) | Functional Value<br>$x_0 = f(x_1 \ x_2 \ x_3)$ |
|----------------------------------------|------------------------------------------------|
| 0 0 0                                  | 1                                              |
| 0 0 1                                  | 1                                              |
| 0 1 0                                  | 0                                              |
| 0 1 1                                  | 1                                              |
| 1 0 0                                  | 0                                              |
| 1 0 1                                  | 0                                              |
| 1 1 0                                  | 1                                              |
| 1 1 1                                  | 0                                              |

lower half) of the truth table can display all the information for a function generating only cycles.

#### B. HALF TRUTH TABLE

Focusing on equation (2), since  $x_n$  is always 1 in the lower half this can be viewed as complementing the functional values for  $g(x_1 \dots x_{n-1})$  in the upper half. In this manner the half truth table in Table 4.2 is constructed for the same de Bruijn sequence (00011101) to aid comparison with Table 4.1. From this point on the term truth table will always mean the upper half truth table with  $x_n = 0$ , unless noted otherwise.

TABLE 4.2  
HALF TRUTH TABLE OF (00011101)

| $x_2$ | $x_1$ | $g(x_1 x_2)$ |
|-------|-------|--------------|
| 0     | 0     | 1            |
| 0     | 1     | 1            |
| 1     | 0     | 0            |
| 1     | 1     | 1            |

The string of functional values in the truth table is defined to be the generator  $G = \{g_0 g_1 \dots g_{2^{n-1}-1}\}$  where the subscripts of  $g$  are the decimal equivalent of  $x_{n-1} \dots x_1$ . Both the weight and parity of generator  $G$  will be of interest as the investigation of this paper continues. Whenever the parity or weight of the truth table is mentioned in this paper, it is referring to the generator of that truth table.

#### C. ZERO TRUTH TABLE

The zero truth table is defined as the truth table in which all functional values are zero. The zero truth table for  $n = 3$  contained in Table 4.3 is basically the output of a circulating register which generates pure cycles.

Pure cycles are defined as cyclic permutations of the original state. The zero truth table in Table 4.3 generates the four pure cycles shown in Fig. 4.1. The number of pure

TABLE 4.3  
ZERO TRUTH TABLE FOR  $n = 3$

| $x_2$ | $x_1$ | $g(x_1, x_2)$ |
|-------|-------|---------------|
| 0     | 0     | 0             |
| 0     | 1     | 0             |
| 1     | 0     | 0             |
| 1     | 1     | 0             |

cycles  $Z_n$  has been shown [Ref. 7: p. 120] to be

$$Z_n = \frac{1}{n} \sum_{d|n} \phi(d) 2^{n/d}.$$

Eulers totient function  $\phi(d)$  is the number of fractions of the form  $a/d$  where  $1 \leq a \leq d$  and  $a/d$  is in lowest terms. The summation is over all positive integers  $d$  which divide  $n$ , denoted  $(d|n)$ . It is further shown [Ref. 5] that  $Z_n^{-1}$  is the minimum possible weight truth table that can generate a de Bruijn sequence.

In the next section, the proof of theorem 6 gives an example of how pure cycles can be joined in a way to create a de Bruijn sequence that has a minimum weight truth table. Table 4.5 gives a listing of  $Z_n$  and  $Z_n^{-1}$  for  $1 \leq n \leq 7$ .

#### D. ONES TRUTH TABLE

The ones truth table assigns a functional value of 1 to every entry of  $g(x_1 \cdots x_{n-1})$ . The ones truth table depicts the output of a complementing shift register. The input is

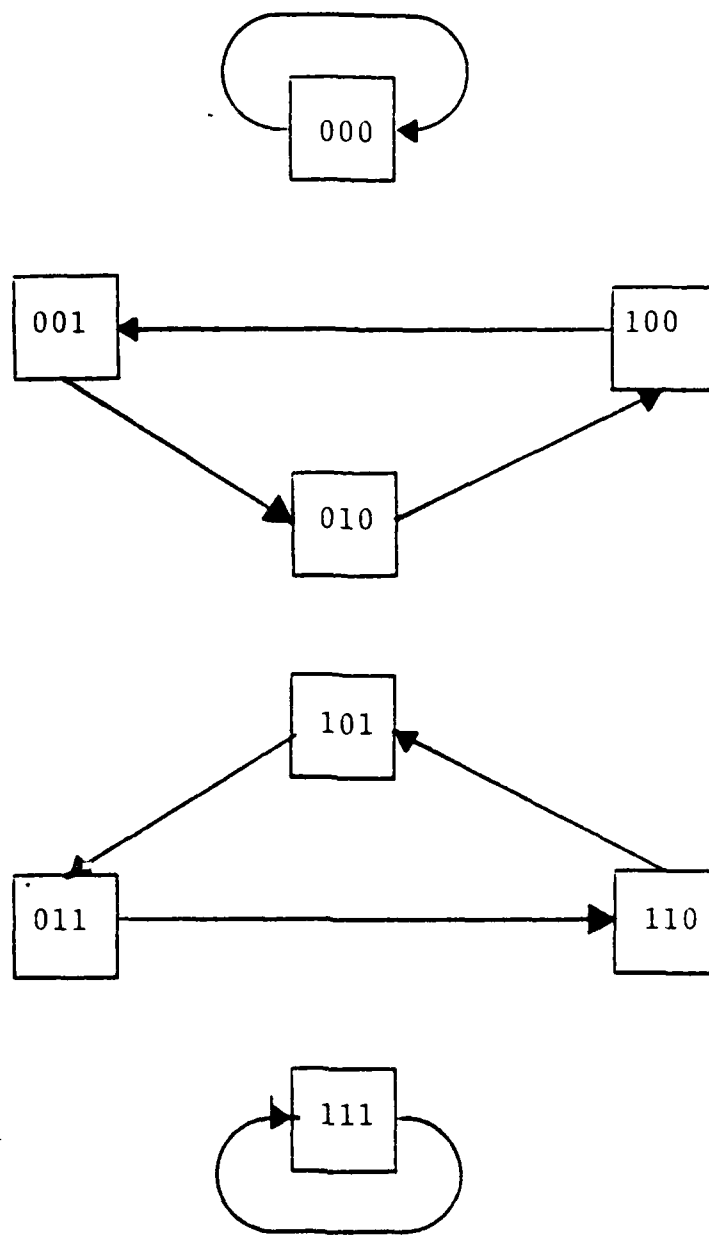


Fig. 4.1 Pure Cycles ( $n=3$ ).

always the complement of the output, i.e.  $f(x_1 \dots x_n) = 1 + x_n$ . The ones truth table for  $n = 3$  is shown in Table 4.4. The complementing cycles from Table 4.4 are depicted in Fig. 4.2.

TABLE 4.4  
ONES TRUTH TABLE ( $n = 3$ )

| $x_2$ | $x_1$ | $g(x_1, x_2)$ |
|-------|-------|---------------|
| 0     | 0     | 1             |
| 0     | 1     | 1             |
| 1     | 0     | 1             |
| 1     | 1     | 1             |

The number of complementing cycles  $z_n^*$  [Ref. 7] is

$$z_n^* = \frac{z_n}{2} - \frac{1}{2n} \sum_{2d|n} \phi(2d) 2^{\frac{n}{2d}}.$$

Since summation for  $z_n^*$  is over all  $2d$  (even) numbers which divide  $n$ , for  $n$  odd  $z_n^* = \frac{z_n}{2}$ .

Accordingly Fredricksen [Ref. 5] shows truth tables of max weight that can generate a de Bruijn sequence is

$$2^{n-1} - z_n^* + 1.$$

The values of  $z_n^*$  and  $2^{n-1} - z_n^* + 1$  are given in Table 4.5 for  $1 \leq n \leq 7$ . Also included are the number of de Bruijn sequences having truth tables of maximum or minimum weight from a listing by Fredricksen [Ref. 5].

TABLE 4.5  
PURE CYCLE COMPILATION

| <u>n</u> | <u>Z<sub>n</sub></u> | <u>Z<sub>n</sub>-1</u> | # de Bruijn<br>Sequences<br>with Min<br>Wt Truth Table | <u>Z<sub>n</sub>*</u> | <u>2<sup>n-1</sup>-Z<sub>n</sub>*+1</u> | # de Bruijn<br>Sequences<br>with Max<br>Wt Truth Table |
|----------|----------------------|------------------------|--------------------------------------------------------|-----------------------|-----------------------------------------|--------------------------------------------------------|
| 1        | 2                    | 1                      | 1                                                      | 1                     | 1                                       | 1                                                      |
| 2        | 3                    | 2                      | 1                                                      | 1                     | 2                                       | 1                                                      |
| 3        | 4                    | 3                      | 2                                                      | 2                     | 3                                       | 2                                                      |
| 4        | 6                    | 5                      | 12                                                     | 2                     | 7                                       | 3                                                      |
| 5        | 8                    | 7                      | 2 <sup>6</sup> .3 <sup>2</sup>                         | 4                     | 13                                      | 2 <sup>6</sup>                                         |
| 6        | 14                   | 13                     | 2 <sup>14</sup> .3 <sup>4</sup> .5 <sup>2</sup>        | 6                     | 27                                      | 2 <sup>14</sup>                                        |
| 7        | 20                   | 19                     | 2 <sup>28</sup> .3 <sup>5</sup> .5 <sup>3</sup> .13    | 10                    | 55                                      | 2 <sup>26</sup> .3                                     |

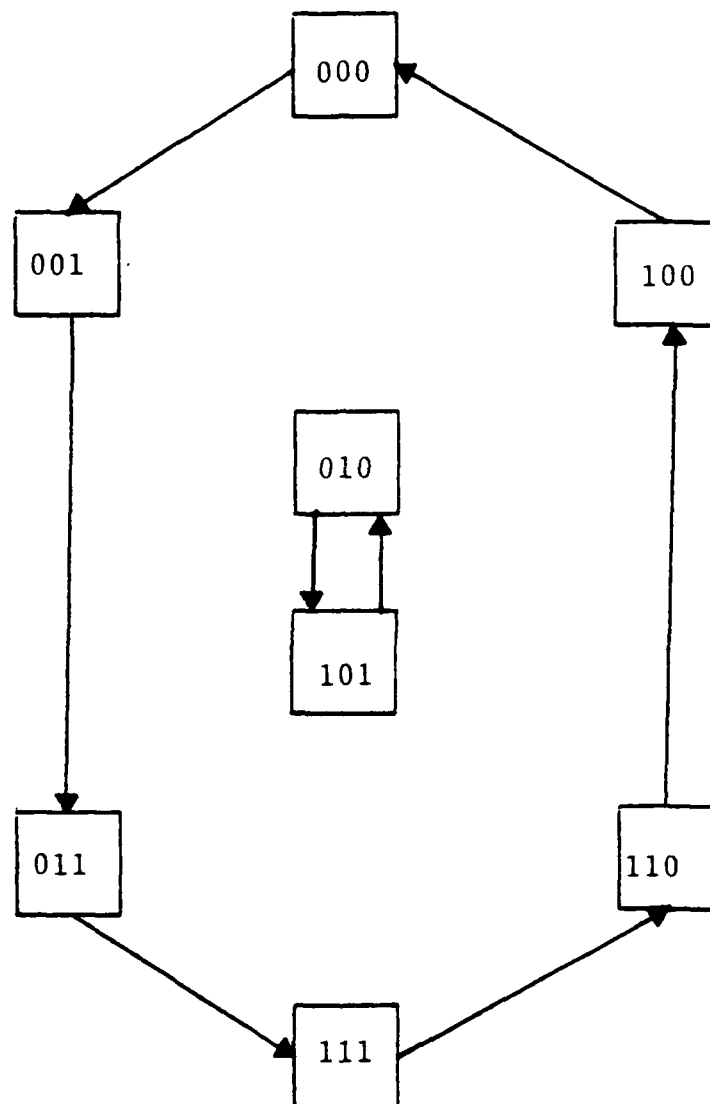


Fig. 4.2 Complementing Cycles ( $n=3$ )

#### E. EFFECTS OF CHANGING THE TRUTH TABLE

If the ones truth table in Table 4.4 is changed so that  $g(0,1) = 0$  vice 1, the truth table of Table 4.6 is produced.

TABLE 4.6  
TRUTH TABLE (TABLE 4.4 MODIFIED)

| $x_2$ | $x_1$ | $g(x_1 x_2)$ |
|-------|-------|--------------|
| 0     | 0     | 1            |
| 0     | 1     | 0            |
| 1     | 0     | 1            |
| 1     | 1     | 1            |

This change in the truth table effects the cycles of Fig. 4.2 by joining them as depicted in Fig. 4.3. Indeed the change produces a Hamiltonian path for the de Bruijn sequence (00010111).

Suppose the truth table of Table 4.6 is now changed so that  $g(00) = 0$  vice 1. This produces the truth table in Table 4.7, and its cyclic composition in Fig. 4.4.

TABLE 4.7  
TRUTH TABLE (TABLE 4.6 MODIFIED)

| $x_2$ | $x_1$ | $g(x_1 x_2)$ |
|-------|-------|--------------|
| 0     | 0     | 0            |
| 0     | 1     | 0            |
| 1     | 0     | 1            |
| 1     | 1     | 1            |

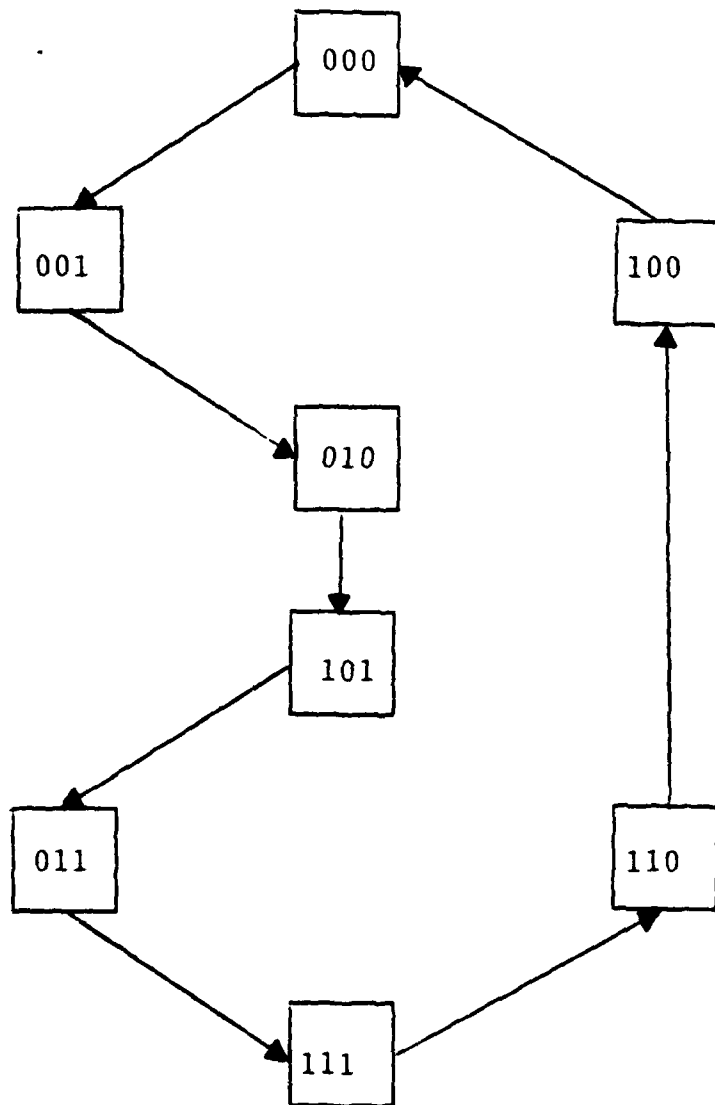


Fig. 4.3 Cyclic Composition of Table 4.4.

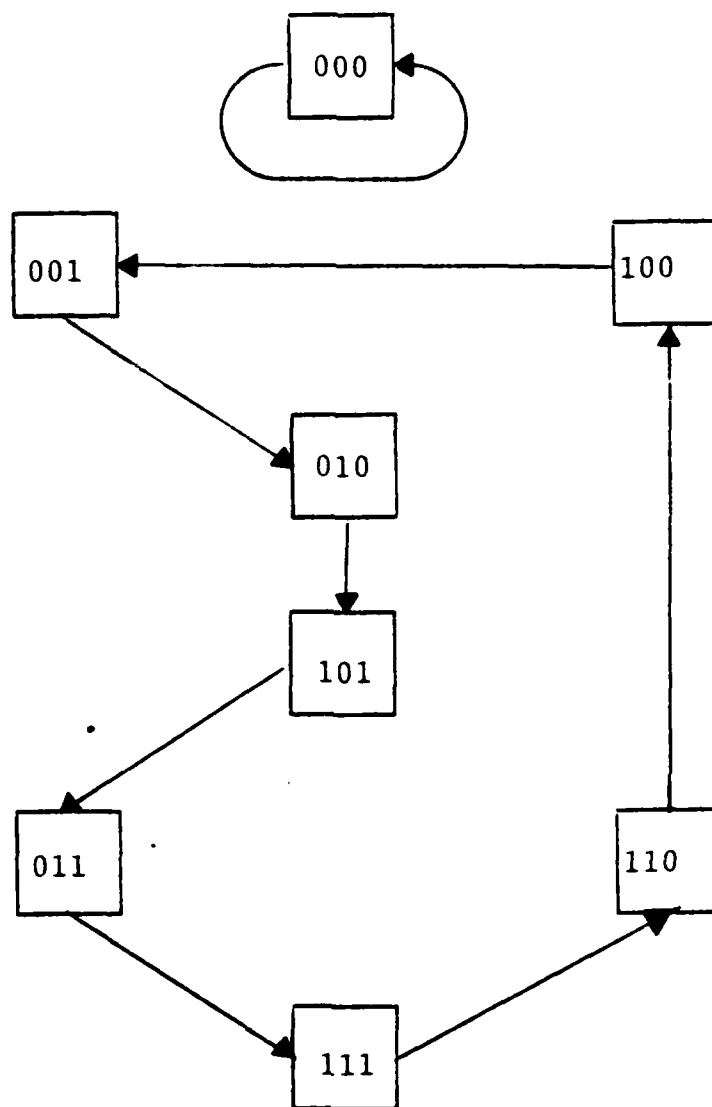


Fig. 4.4 Cyclic Composition of Table 4.7.

This change in the truth table causes the cycle to split into two cycles. Suppose  $(x_n \cdots x_1)$  is an element on upper of two cycles as shown in Fig. 4.5 and that its successor is

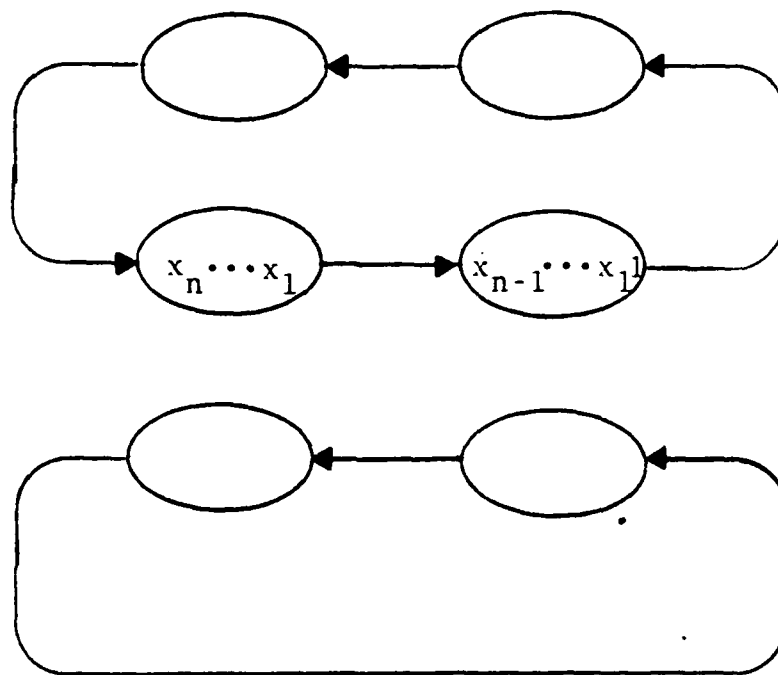


Fig. 4.5 Two Cycle Graph.

$x_{n-1} \cdots x_1 1$  as  $f(x_1 \cdots x_n) = 1$ . If the truth table is now changed so that  $f(x_1 \cdots x_n) = 0$ , then  $x_{n-1} \cdots x_1 0$  is the new successor for  $x_n \cdots x_1$ . Retaining the cycles only condition  $f(x_1 \cdots x_{n-1} \bar{x}_n)$  must now be 1. So the successor of  $\bar{x}_n x_{n-1} \cdots x_1$  is now  $x_{n-1} \cdots x_1 1$ . One of two things can happen how depending on whether  $x_{n-1} \cdots x_1 0$  is on the upper or lower cycle.

First if  $(x_{n-1} \cdots x_1 0)$  is on the upper cycle, then that cycle is split as shown in Fig. 4.6 forming three cycles.

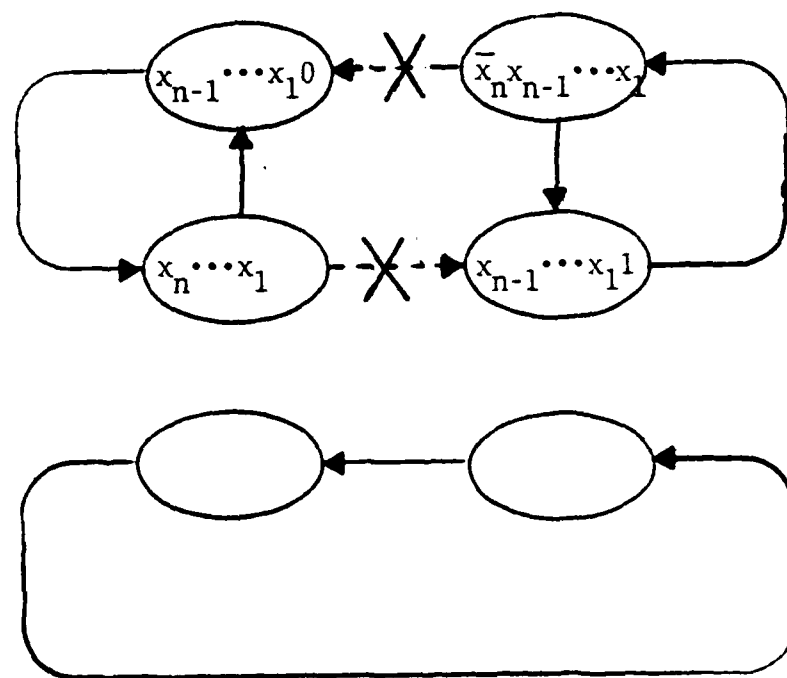


Fig. 4.6 Cycle Splitting.

Otherwise if  $(x_{n-1} \cdots x_1 0)$  is on the lower cycle, then those two cycles are joined as shown in Fig. 4.7.

Clearly the parity of the cycles changes for each change in the truth table. The following theorem from Golomb [Ref. 7: p. 122] shows that the parity of the number of cycles and the parity of the truth table generator are equal.

Theorem 3. For  $n > 2$ , the parity of the truth table is equal to the parity of the number of cycles of the truth table.

Since a de Bruijn sequence is one cycle by definition, the following corollary of theorem 3 is given.

Corollary. If a sequence is de Bruijn, then the parity of the TT of that sequence is odd.

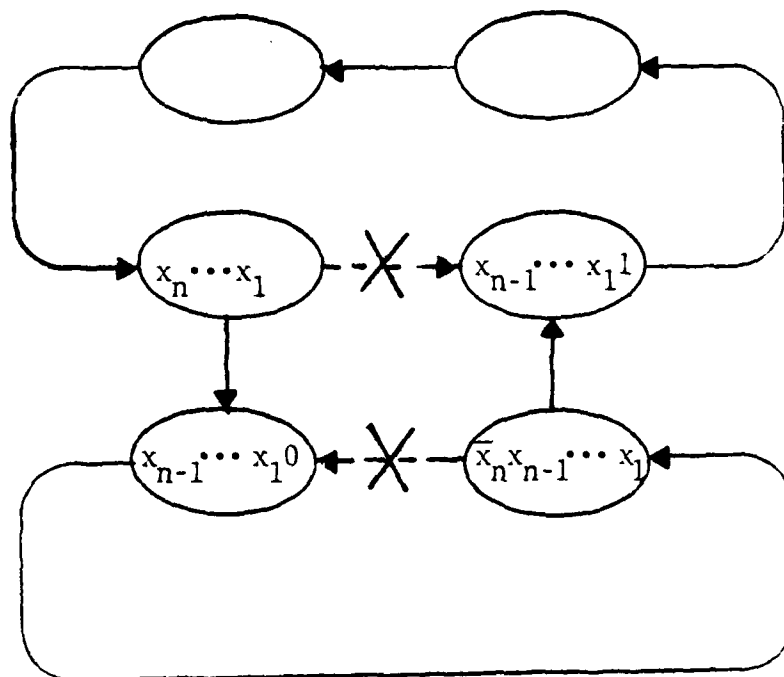


Fig. 4.7 Cycle Joining.

#### F. SPECIAL NUMBERS

Analyzing the effects of de Bruijn sequence operators on their truth tables, certain binary numbers are found to have special properties which can be exploited in later analysis.

### 1. Type RC Numbers

If  $X = x_1 \cdots x_n$  is a binary number, such that  $\bar{x}_n \cdots \bar{x}_1 = x_1 \cdots x_n$  then  $X$  is called a RC<sub>n</sub> number.

Lemma 4. For  $n$  even there are exactly  $2^{\frac{n}{2}}$  type RC numbers.

Proof. For  $n$  even, if  $X$  is an RC number, then

$x_1 \cdots x_n = \bar{x}_n \cdots \bar{x}_1$  by definition. Therefore,  
 $x_1 = \bar{x}_n, x_2 = \bar{x}_{n-1}$ , etc. Thus  $x_1 \cdots x_n$  can be written as  
 $x_1 x_2 \cdots x_{\frac{n}{2}} \bar{x}_{\frac{n}{2}} \cdots \bar{x}_2 \bar{x}_1$ . Since  $\frac{n}{2}$  positions can be filled in  
 either of two ways, the total number of RC numbers for  $n$   
 even is  $2^{\frac{n}{2}}$ .

Q.E.D.

There are no type RC numbers for  $n$  odd, since this would require that  $x_{\frac{n+1}{2}} = \bar{x}_{\frac{n+1}{2}}$  which is impossible.

### 2. Type R Numbers

If  $X = x_1 \cdots x_n$  is a binary number such that  $x_1 \cdots x_n = x_n \cdots x_1$ , then it is called a type R<sub>n</sub> number.

Lemma 5. For  $n$  even there are exactly  $2^{\frac{n+1}{2}}$  type R numbers, and for  $n$  odd there are exactly  $2^{\frac{n+1}{2}}$  type R numbers.

Proof. The proof for  $n$  even parallels that of Lemma 4 and will not be repeated. For  $n$  odd, since  $x_{\frac{n+1}{2}} = x_{\frac{n+1}{2}}$  there are  $\frac{n+1}{2}$  positions to be filled in either of two ways. Therefore, for  $n$  odd there are exactly  $2^{\frac{n+1}{2}}$  type R numbers.

Q.E.D.

A useful way of organizing special numbers and other truth table values to assist in evaluating effects on the generators for various operators is shown in Table 4.8 for  $n = 5$  and  $n = 6$ . The numbers are the decimal equivalent of the binary  $(n-1)$ -tuple,  $x_{n-1} \cdots x_1$ , from the feedback function

$$x_0 = x_n + g(x_1 \cdots x_{n-1})$$

which also corresponds to the truth table state.

For example for  $n = 5$ , if  $f(2) = 1$  for some sequence  $S$  then:  $f(11) = 1$  for  $r \bar{S}$ ,  $f(4) = 1$  for  $r S$ , and  $f(13) = 1$  for  $\bar{S}$ . In general, for some operator  $\beta$  and some number  $a$ , if  $f(a) = 1$  for some sequence  $S$ , then  $f(\beta a) = 1$  for  $\beta S$ . Special numbers have properties in addition to this. If  $\alpha$  is a type RC number and  $f(\alpha) = 1$  for  $S$ , then  $f(\alpha) = f(r \bar{\alpha}) = 1$  for  $r \bar{S}$ . Similarly if  $\gamma$  is a type R number and  $f(\gamma) = 1$  for  $S$ , then  $f(\gamma) = f(r\gamma) = 1$  for  $r S$ . Thus, if we want to show  $S$  is a sequence such that  $S = r \bar{S}$ , then if  $f(a) = 1$  in  $S$ , then  $f(r \bar{a}) = 1$  in  $S$  also.

#### G. GENERATOR ANALYSIS

Analysis of the generators for the de Bruijn sequences  $S$ ,  $r S$ ,  $\bar{S}$ , &  $r \bar{S}$  in Table 4.9 appears to indicate the generator  $G$  of sequence  $\bar{S}$  denoted  $G(\bar{S})$  is the reverse of the generator  $G(S)$ . Notice also that  $G(r S) = r [G(r \bar{S})]$  for  $S$ . Although Table 4.9 is an example of a single sequence  $S$ , it is not an isolated incident; in general the result  $G(S) = r [G(\bar{S})]$  holds and is proven in the following theorem.

TABLE 4.8  
TRUTH TABLE ANALYSIS CHART

| S           | $\bar{S}$   | rS          | r $\bar{S}$ |                            |
|-------------|-------------|-------------|-------------|----------------------------|
| $\bar{S}$   | S           | r $\bar{S}$ | rS          |                            |
| rS          | r $\bar{S}$ | S           | $\bar{S}$   |                            |
| r $\bar{S}$ | rS          | $\bar{S}$   | S           |                            |
| 0           | 15          | 0           | 15          | ← Truth table states (n=5) |
| 1           | 14          | 8           | 7           | Type R numbers             |
| 2           | 13          | 4           | 11          | (0,6,9,15)                 |
| 3           | 12          | 12          | 3           | Type RC numbers            |
| 5           | 10          | 10          | 5           | (3,5,10,12)                |
| 6           | 9           | 6           | 9           |                            |
| 0           | 31          | 0           | 31          | ← Truth table states (n=6) |
| 1           | 30          | 16          | 15          | Type R numbers             |
| 2           | 29          | 8           | 23          | (0,4,10,31)                |
| 3           | 28          | 24          | 7           | Type RC numbers            |
| 4           | 27          | 4           | 27          | (None)                     |
| 5           | 26          | 20          | 11          |                            |
| 6           | 25          | 12          | 19          |                            |
| 9           | 22          | 18          | 13          |                            |
| 10          | 21          | 10          | 21          |                            |
| 14          | 17          | 14          | 17          |                            |

TABLE 4.9  
GENERATOR ANALYSIS FOR de BRUIJN SEQUENCES  
( $rS \neq \bar{S}$ )

S    11111001000111011010011000001010  
 $\bar{S}$     11111010100000110111000100101100  
rS    11111010100000110010110111000100  
 $r\bar{S}$     11111001101001000111011000001010

|                                                                                     | $x_{n-1}, \dots, x_1$                                                               | G (S) | G ( $\bar{S}$ ) | G (rS)   | G ( $r\bar{S}$ ) |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------|-----------------|----------|------------------|
|                                                                                     | 0                                                                                   | 1     | 1               | 1        | 1                |
|                                                                                     | 1                                                                                   | 0     | 1               | 1        | 0                |
|                                                                                     | 2                                                                                   | 1     | 0               | 0        | 1                |
|   |   | 1     | 0               | 0        | 1                |
| Type RC                                                                             | 4                                                                                   | 0     | 1               | 1        | 0                |
|                                                                                     |  | 0     | 1               | 1        | 0                |
|  |  | 0     | <u>1</u>        | 0        | 1                |
| Type R                                                                              | 7                                                                                   | 0     | 1               | 1        | 0                |
| (other than                                                                         | 8                                                                                   | 1     | 0               | 0        | 1                |
| 0 & 15)                                                                             |  | 1     | 0               | <u>1</u> | 0                |
|                                                                                     |  | 1     | 0               | 0        | 1                |
|                                                                                     | 11                                                                                  | 1     | 0               | 0        | 1                |
|                                                                                     |  | 0     | 1               | 1        | 0                |
|                                                                                     | 13                                                                                  | 0     | 1               | 1        | 0                |
|                                                                                     | 14                                                                                  | 1     | 0               | 0        | 1                |
|                                                                                     | 15                                                                                  | 1     | 1               | 1        | 1                |

Theorem 4: If  $S$  is a de Bruijn sequence with generator  $G(S)$ , then  $\bar{S}$  is a de Bruijn sequence with generator  $r[G(S)]$ .

Proof: Let  $G(S) = \{g_1, g_2, \dots, g_{2^{n-1}}\}$  then the full truth table for  $S$  is given in Table 4.10.

TABLE 4.10  
FULL TRUTH TABLE FOR  $S$

| $x_n$    | $x_{n-1}$ | $x_{n-2}$ | $\dots$ | $x_1$    | $f(x_1, \dots, x_n)$ |
|----------|-----------|-----------|---------|----------|----------------------|
| 0        | 0         | 0         | $\dots$ | 0        | $g_1$                |
| 0        | 0         | 0         | $\dots$ | 1        | $g_2$                |
| $\vdots$ |           |           |         | $\vdots$ | $\vdots$             |
| 0        | 1         | 1         | $\dots$ | 1        | $g_{2^{n-1}}$        |
| <hr/>    |           |           |         |          | <hr/>                |
| 1        | 0         | 0         | $\dots$ | 0        | $\bar{g}_1$          |
| 1        | 0         | 0         | $\dots$ | 1        | $\bar{g}_2$          |
| $\vdots$ |           |           |         |          | $\vdots$             |
| 1        | 1         | 1         | $\dots$ | 1        | $\bar{g}_{2^{n-1}}$  |

If  $x_n, x_{n-1}, \dots, x_1, f(x_1 \dots x_n)$  is a  $(n+1)$  long string in  $S$ , then  $\bar{x}_n, \bar{x}_{n-1}, \dots, \bar{x}_1, \overline{f(x_1 x_2 \dots x_n)}$  is a  $(n+1)$  long string in  $\bar{S}$ .

Therefore we can transform each line of the full truth table for  $S$  by taking its complement to get Table 4.11.

TABLE 4.11  
FULL TRUTH TABLE FOR  $\bar{S}$  (NON STANDARD)

| $x_n$    | $x_{n-1}$ | $x_{n-2}$ | $\dots$  | $x_1$ | $f(x_1, x_2, \dots, x_n)$ |
|----------|-----------|-----------|----------|-------|---------------------------|
| 1        | 1         | 1         | $\dots$  | 1     | $\bar{g}_1$               |
| 1        | 1         | 1         | $\dots$  | 0     | $\bar{g}_2$               |
| $\vdots$ |           |           | $\ddots$ |       | $\vdots$                  |
| 1        | 0         | 0         | $\dots$  | 0     | $\bar{g}_{2^{n-1}}$       |
| 0        | 1         | 1         | $\dots$  | 1     | $g_1$                     |
| 0        | 1         | 1         | $\dots$  | 0     | $g_2$                     |
| $\vdots$ |           |           | $\ddots$ |       | $\vdots$                  |
| 0        | 0         | 0         | $\dots$  | 0     | $g_{2^{n-1}}$             |

Rearranging the rows from top to bottom, the TT for  $\bar{S}$  is placed in standard form as depicted in the Table 4.12. Further examination of the generators in Table 4.9 shows the structure of  $G(\bar{S})$  to be remarkably similar to the structure of  $G(rS)$ , with the exception that the functional values of type R numbers (6 & 9) are transposed. If, however, these values should be the same then clearly  $G(\bar{S}) = G(rS)$  or  $S = r\bar{S}$ . Indeed, this occurs twice for  $n = 3$  and 64 times for  $n = 5$ , and will be shown to happen for all odd  $n \geq 3$ . This cannot happen for  $n$  even, because there are no type RC numbers in the truth table.

TABLE 4.12  
FULL TRUTH TABLE FOR  $\bar{S}$

| $x_n$    | $x_{n-1}$ | $x_{n-2}$ | $\dots$  | $x_1$ | $f(x_1, x_2, \dots, x_n)$ |
|----------|-----------|-----------|----------|-------|---------------------------|
| 0        | 0         | 0         | $\dots$  | 0     | $g_{2^{n-1}}$             |
| $\vdots$ |           |           | $\ddots$ |       | $\vdots$                  |
| 0        | 1         | 1         | $\dots$  | 0     | $g_2$                     |
| 0        | 1         | 1         | $\dots$  | 1     | $g_1$                     |
| 1        | 0         | 0         | $\dots$  | 0     | $\bar{g}_{2^{n-1}}$       |
| $\vdots$ |           |           | $\ddots$ |       | $\vdots$                  |
| 1        | 1         | 1         | $\dots$  | 0     | $\bar{g}_2$               |
| 1        | 1         | 1         | $\dots$  | 1     | $\bar{g}_1$               |

Clearly  $G(\bar{S})$  is  $r[G(S)]$

Q.E.D.

## V. RESULTS

Examining Table 3.2 it can be quickly determined that the number of de Bruijn sequences of given complexity for  $3 \leq n \leq 6$  is  $0 \pmod{4}$ . Games and Chan [Ref. 1] made this conjecture, but were able to show only that the distribution  $\alpha(c, n)$  was  $0 \pmod{2}$ . Their result followed by showing that for a given de Bruijn sequence  $S$  of complexity  $c$ , there existed a unique de Bruijn sequence  $\bar{S}$  also having complexity  $c$ . In Section III it was shown that reverse and reverse dual operators preserve the complexity of de Bruijn sequences as well.

If each of these new operators produced unique de Bruijn sequences, then it would be easy to show that the numbers  $\alpha(c, n) \equiv 0 \pmod{4}$  since for every de Bruijn sequence  $S$  there would also exist  $\bar{S}$ ,  $r S$  and  $r \bar{S}$  all de Bruijn and unique having complexity  $c$ . As mentioned in Section IV, the sequences  $r \bar{S}$  and  $r S$  are not always distinct from the sequences  $S$  &  $\bar{S}$  respectively; however, for  $n$  even the next theorem shows that all four of these sequences are distinct. In addition it will be shown that RC sequences occur for all  $n$  odd, and a lower bound for the number of RC sequences will be established for all  $n$  and investigated for  $n = 7$ .

A.  $\alpha(c, n) \equiv 0 \text{ MODULO } 4 \text{ FOR } n \text{ EVEN}$

Etzion and Lempel [Ref. 6] give a proof that  $\alpha(c, n)$  is congruent to 0 mod 4 for  $c, n$  even. In the proof for  $n$  even given here a different approach is taken.

Theorem 5. For even  $n \geq 3$ , the numbers  $\alpha(c, n) \equiv 0 \pmod{4}$  for a de Bruijn sequence  $S$  of span  $n$  and complexity  $c$ .

Proof. From theorem 1, it is known that for a de Bruijn sequence  $S$  of complexity  $c$ , that  $\bar{S}$ ,  $rS$  &  $r\bar{S}$  also have complexity  $c$ . Games and Chan showed the uniqueness of  $\bar{S}$ , so all that remains is to show that  $rS$  is distinct from  $S$ , or equivalently that  $r\bar{S}$  is distinct from  $S$  for  $n$  even.

Suppose on the contrary that  $S = r\bar{S}$ . Then consider an  $n$ -tuple  $0a_{n-1} \cdots a_1$  in the truth table such that  $f(a_1 \cdots a_{n-1} 0) = 1$ . Then  $0a_{n-1} \cdots a_1 1$  is a  $n+1$  long string in  $S$ , and  $0\bar{a}_1 \cdots \bar{a}_{n-1} 1$  is a  $n+1$  long string in  $r\bar{S}$ . If  $S = r\bar{S}$  then  $0\bar{a}_1 \cdots \bar{a}_{n-1} 1$  is a  $n+1$  long string in  $S$ , which implies that  $1\bar{a}_1 \cdots \bar{a}_{n-1} 0$  is a  $n+1$  long string in  $S$ , and therefore  $f(\bar{a}_1 \cdots \bar{a}_{n-1} 0) = 1$ . This must hold for every  $x_1 \cdots x_{n-1} 0$  such that  $f(x_1 \cdots x_{n-1} 0) = 1$ . Pairing these vectors,  $a_1 \cdots a_{n-1}$  and  $\bar{a}_{n-1} \cdots \bar{a}_1$ , two at a time results in an even number of 1's in the truth table. So there must be a vector which pairs with itself as the parity of ones is odd. But then  $x_{n-1} \cdots x_1 = \bar{x}_1 \cdots \bar{x}_{n-1}$  is a

contradiction since  $\bar{x}_{\frac{n+1}{2}} \neq x_{\frac{n+1}{2}}$  for  $n$  even. Therefore for  $n$  even  $S \neq r \bar{S}$  and  $r S \neq \bar{S}$ , so  $r S$  and  $r \bar{S}$  are distinct and  $\alpha(c, n) \equiv 0 \pmod{4}$ .

Q.E.D.

#### B. RC SEQUENCES EXIST FOR ALL ODD $n \geq 3$

The results  $\alpha(c, n) \equiv 0 \pmod{4}$  for all  $n$  are not obtained as hoped for. For  $n = 3$  and  $n = 5$  RC sequences are known to exist, but it is not known if this is true for all odd  $n \geq 3$  or just some. The following theorem shows that RC sequences exist for all odd  $n \geq 3$ . Recall that RC sequences are those sequences  $S$  for which  $S = r \bar{S}$  or equivalent by  $\bar{S} = r S$  since  $r(S) = r(r \bar{S})$  yields  $\bar{S} = r S$ .

Lemma 6. The sequence formed by joining all pure cycles of  $n$ -tuples is de Bruijn.

Proof. The least elements of each pure cycle for a given  $n$  are easily composed and arranged in order by weight according to the algorithm in Appendix A. Since the pure cycles contain all  $n$ -tuples exactly once, all that remains is to show how each pure cycle can be interconnected, thus forming a de Bruijn sequence. For each cycle of wt  $a \geq 1$  there exists a least element " $2X+1$ " (necessarily odd, if it were even ( $2X$ ) then " $X$ " is on the same cycle and smaller) whose predecessor " $X$ " has wt  $(a-1)$ . Since the pure cycles are ordered by weight, it is clear that the least element of each pure cycle of wt  $a \geq 1$  can be joined to a cycle of

wt  $(a-1)$  by changing the truth table for its predecessor, i.e.  $g(X)$  becomes 1. In this way all the pure cycles are now interconnected, and the sequence is de Bruijn.

Q.E.D.

Theorem 6. For all odd  $n \geq 3$ , there exist RC de Bruijn sequences.

Proof. An RC de Bruijn sequence can always be composed in the following way for  $n \geq 3$ . First construct a light cycle (LC) for those pure cycles of wt  $\leq \frac{n-1}{2}$  identical to the method used in Lemma 6. Note that when the cycles of wt  $\frac{n-1}{2}$  are joined to cycles of smaller weight the truth table is changed at positions whose weight is less than  $\frac{n-1}{2}$ . For every  $X$  such that  $f(X) = 1$  in LC, induce  $f(rX) = 1$  on the pure cycles of wt  $(n-a) \geq \frac{n+1}{2}$ , forming a heavy cycle (HC). Note that HC is the reverse complement of LC. All of the positions changed so that  $g(X) = 1$  on HC are of weights bigger than or equal to  $\frac{n+1}{2}$ .

Join LC and HC by using a type RC number,  $y$ , which exist by Lemma 4, since for  $n$  odd the truth table states have even  $(n-1)$  length. The RC number  $y$  has weight  $\frac{n-1}{2}$ . Letting  $f(Y) = 1$  then joins LC and HC forming one sequence. By Theorem 1 the sequence is RC, and by Lemma 6 the sequence is de Bruijn.

Q.E.D.

## C. LOWER BOUND ON NUMBER OF RC SEQUENCES

### 1. Theorem

A weak lower bound on the number of RC de Bruijn sequences is established.

Theorem 7: A lower bound on the number of de Bruijn RC sequences for odd  $n \geq 3$  is  $A \cdot 2^{\frac{n-1}{2}}$ , where A is the number of possible different interconnections for pure cycles of weight  $\leq \frac{n-1}{2}$  as determined by the Best method [Ref. 5].

Proof: Restricting attention to those cycles of  $wt \leq \frac{n-1}{2}$  (since the other connections are induced), the Best method gives the number A of possible different interconnections for the pure cycles of weight  $\leq \frac{n-1}{2}$ . Since there exist  $2^{\frac{n-1}{2}}$  type RC numbers, this gives  $2^{\frac{n-1}{2}}$  ways of joining A different pairs of cycles for a total of  $A \cdot 2^{\frac{n-1}{2}}$  possibilities.

Q.E.D.

### 2. Example for $n = 7$

The pure cycles of  $wt \leq 3$  and the adjacency matrix of A are given in Tables 5.3 and 5.4 respectively. The value of the determinant of the adjacency matrix is 38,880 for any diagonal element. This gives a lower bound of  $38,880 \times 8 = 311,040$  for the number of de Bruijn RC sequences.

TABLE 5.1  
PURE CYCLES FOR  $N=7$  &  $wt \leq 3$

|    |    |    |     |     |     |    |
|----|----|----|-----|-----|-----|----|
| 0  |    |    |     |     |     |    |
| 1  | 2  | 4  | 8   | 16  | 32  | 64 |
| 3  | 6  | 12 | 24  | 48  | 96  | 65 |
| 5  | 10 | 20 | 40  | 80  | 33  | 66 |
| 7  | 14 | 28 | 56  | 112 | 97  | 67 |
| 9  | 18 | 36 | 72  | 17  | 34  | 68 |
| 11 | 22 | 44 | 88  | 49  | 98  | 69 |
| 13 | 26 | 52 | 104 | 81  | 35  | 70 |
| 19 | 38 | 76 | 25  | 50  | 100 | 73 |
| 21 | 42 | 84 | 41  | 82  | 37  | 74 |

TABLE 5.2  
ADJACENCY MATRIX FOR  $n=7$

|    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|
| 1  | -1 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| -1 | 7  | -2 | -2 | -2 | 0  | 0  | 0  | 0  | 0  |
| 0  | -2 | 7  | 0  | 0  | -2 | -1 | -1 | -1 | 0  |
| 0  | -2 | 0  | 7  | 0  | -1 | -1 | -1 | 0  | -2 |
| 0  | -2 | 0  | 0  | 7  | 0  | -1 | -1 | -2 | -1 |
| 0  | 0  | -2 | -1 | 0  | 3  | 0  | 0  | 0  | 0  |
| 0  | 0  | -1 | -1 | -1 | 0  | 3  | 0  | 0  | 0  |
| 0  | 0  | -1 | -1 | -1 | 0  | 0  | 3  | 0  | 0  |
| 0  | 0  | -1 | 0  | -2 | 0  | 0  | 0  | 3  | 0  |
| 0  | 0  | 0  | -2 | -1 | 0  | 0  | 0  | 0  | 3  |

## VI. CONJECTURES

Although a complete proof for  $\alpha(c, n) \equiv 0 \pmod{4}$  has yet to be given, a technique for grouping RC sequences in a  $0 \pmod{4}$  fashion will be demonstrated for  $n = 5$ . However, the technique fails to preserve complexity in every case. However, for  $n = 5$  the complexities produced were congruent to  $0 \pmod{2}$  and when the complement of each sequence is added a  $0 \pmod{4}$  distribution results. It remains, however, that the complexity of the generated sequences are not determined apriori. The technique presented is interesting in its own right, and it is hoped that the interested reader may be able to apply it towards a solution of the  $0 \pmod{4}$  distribution.

### A. RC SEQUENCE GENERATOR TECHNIQUE

Table 6.1 shows a listing of four RC sequences and their generators. The technique used was to choose in turn each of the type RC numbers to have a functional value of 1.

Note that the complexity of  $S_3$  and  $S_5$  are both 23, while the complexity of  $S_{10}$  and  $S_{12}$  are both 29. At present there is no way of knowing which pair of RC sequences will have the same complexity, except that it appears  $C(S_k) = C(S_{r\bar{k}})$  iff all four RC sequences have the same complexity. A listing of the generators for each of the 32 pairs of RC sequences

TABLE 6.1

## RC GENERATOR TECHNIQUE

|                                                  | $C(S_3)=23$ | $C(S_5)=23$ | $C(S_{10})=29$ | $C(S_{12})=29$ |
|--------------------------------------------------|-------------|-------------|----------------|----------------|
| $n$                                              | $G(S_3)$    | $G(S_5)$    | $G(S_{10})$    | $G(S_{12})$    |
| 0                                                | 1           | 1           | 1              | 1              |
| 1                                                | 1           | 1           | 1              | 1              |
| 2                                                | 0           | 0           | 0              | 0              |
| <span style="border: 1px solid black;">3</span>  | <u>1</u>    | 0           | 0              | 0              |
| 4                                                | 1           | 1           | 1              | 1              |
| <span style="border: 1px solid black;">5</span>  | 0           | <u>1</u>    | 0              | 0              |
| 6                                                | 1           | 1           | 1              | 1              |
| 7                                                | 1           | 1           | 1              | 1              |
| 8                                                | 1           | 1           | 1              | 1              |
| 9                                                | 1           | 1           | 1              | 1              |
| <span style="border: 1px solid black;">10</span> | 0           | 0           | <u>1</u>       | 0              |
| 11                                               | 0           | 0           | 0              | 0              |
| <span style="border: 1px solid black;">12</span> | 0           | 0           | 0              | <u>1</u>       |
| 13                                               | 1           | 1           | 1              | 1              |
| 14                                               | 1           | 1           | 1              | 1              |
| 15                                               | 1           | 1           | 1              | 1              |

indicates RC number.

$S_3 = 11111001010001001101110101100000$

$S_5 = 11111001011000001101110101000100$

$S_{10} = 11111001010110000011011101000100$

$S_{12} = 11111000001101110101100101000100$

is prepared in Table 6.2. These are listed in order by  $W(G)$  and then by complexity as far as the groupings allow. Keep in mind, that the complement of each RC sequence is not included in the table. A close analysis of this table then shows a 0 (mod 4) grouping for the number of RC sequences of complexity  $c$  and span  $n = 5$ .

#### B. PROBLEMS

For  $n = 7$ , there exist 6 type R numbers (other than 0 & 64) and 8 type RC numbers in the truth table. This large number of possibilities will create considerable problems in extending this idea to  $n = 7$  and beyond.

Using this approach a large scale computer based analysis is essential to any further investigation of RC sequences for  $n \geq 7$ . Considering the number of de Bruijn sequences for  $n = 7$  to be  $2^{57}$  or  $1.42 \times 10^{17}$  an algorithm for generating only the RC sequences is crucial, since generating  $10^{17}$  de Bruijn sequences is not technically feasible. Though Theorem 7 establishes the lower bound of 311,040 RC sequences for  $n = 7$ , this is a very weak bound and a presumably still conservative estimate would be on the order of  $10^6$  actual RC sequences for  $n = 7$ .

TABLE 6.2

RC de BRUIJN SEQUENCE 0 (Mod 4)  
GROUPING FOR n=5

| G (S) |          |          |          |      |          |   |          |     |  | W[G(S)] | C(S) |
|-------|----------|----------|----------|------|----------|---|----------|-----|--|---------|------|
| 100   | 0        | 1        | 1        | 1001 | 0        | 0 | <u>1</u> | 101 |  | 7       | 25   |
|       |          |          | 0        |      |          |   | <u>1</u> |     |  | 7       | 25   |
|       |          |          | <u>1</u> |      |          |   | <u>0</u> |     |  | 7       | 27   |
|       | <u>1</u> | <u>0</u> | <u>0</u> |      |          |   |          |     |  | 7       | 27   |
| 100   | <u>0</u> | 0        | 0        | 1011 | <u>1</u> | 0 | 0        | 011 |  | 7       | 27   |
|       |          |          |          |      | <u>0</u> |   | <u>1</u> |     |  | 7       | 27   |
|       | <u>1</u> |          |          |      |          |   | <u>0</u> |     |  | 7       | 29   |
|       | <u>0</u> |          | <u>1</u> |      |          |   |          |     |  | 7       | 29   |
| 101   | 0        | 0        | <u>0</u> | 0010 | 0        | 1 | <u>1</u> | 011 |  | 7       | 31   |
|       |          |          |          |      | <u>1</u> |   | <u>0</u> |     |  | 7       | 31   |
|       |          |          | <u>1</u> |      | <u>0</u> |   |          |     |  | 7       | 31   |
|       | <u>1</u> | <u>0</u> | <u>0</u> |      |          |   |          |     |  | 7       | 31   |
| 100   | <u>0</u> | 1        | 0        | 0010 | 0        | 0 | <u>1</u> | 111 |  | 7       | 31   |
|       |          |          |          |      | <u>1</u> |   | <u>0</u> |     |  | 7       | 31   |
|       |          |          | <u>1</u> |      | <u>0</u> |   |          |     |  | 7       | 31   |
|       | <u>1</u> | <u>0</u> | <u>0</u> |      |          |   |          |     |  | 7       | 31   |
| 101   | <u>0</u> | 0        | 0        | 1011 | <u>1</u> | 1 | 0        | 011 |  | 9       | 31   |
|       |          |          |          |      | <u>0</u> |   | <u>1</u> |     |  | 9       | 31   |
|       | <u>1</u> |          |          |      |          |   | <u>0</u> |     |  | 9       | 31   |
|       | <u>0</u> |          | <u>1</u> |      |          |   |          |     |  | 9       | 31   |
| 100   | 0        | 1        | <u>0</u> | 1011 | <u>1</u> | 0 | 0        | 111 |  | 9       | 31   |
|       |          |          |          |      | <u>0</u> |   | <u>1</u> |     |  | 9       | 31   |
|       | <u>1</u> |          |          |      |          |   | <u>0</u> |     |  | 9       | 31   |
|       | <u>0</u> |          | <u>1</u> |      |          |   |          |     |  | 9       | 31   |
| 111   | 0        | 0        | <u>0</u> | 1111 | <u>1</u> | 1 | 0        | 011 |  | 11      | 23   |
|       |          |          |          |      | <u>0</u> |   | <u>1</u> |     |  | 11      | 23   |
|       | <u>1</u> |          |          |      |          |   | <u>0</u> |     |  | 11      | 29   |
|       | <u>0</u> |          | <u>1</u> |      |          |   |          |     |  | 11      | 29   |
| 101   | 0        | 1        | <u>1</u> | 1011 | 0        | 1 | 0        | 111 |  | 11      | 25   |
|       |          |          | <u>0</u> |      |          |   | <u>1</u> |     |  | 11      | 25   |
|       | <u>1</u> |          |          |      |          |   | <u>0</u> |     |  | 11      | 27   |
|       | <u>0</u> |          |          |      | <u>1</u> |   |          |     |  | 11      | 27   |

## APPENDIX A

### ALGORITHM FOR GENERATING LEAST ELEMENT FOR EVERY PURE CYCLE

This algorithm is designed to produce the least element of each pure cycle. The least elements are initially in decreasing order. A simple rearrangement will group the least elements by weight in decreasing order if necessary. The algorithm to be presented is an adaptation of the  $\theta$ -operation discussed in a paper by Fredricksen and Maiorana [Ref. 10], to generate a lexicographic list of necklaces.

ALGORITHM: Begin the  $\Omega$  operation with the zero  $n$ -tuple, which is the first least element for the zero pure cycle.

$\Omega$  Operation:  $\Omega (x_1 \cdots x_n) = (y_1 \cdots y_n) = Y$

1. Find the largest subscript  $j$  such that  
 $x_j = 0$  and  $x_k = 1$  for  $k > j$ .
2. Form  $x_1 x_2 \cdots x_{j-1} 1$  where  $x_j = 1$
3. Repeat  $x_1 x_2 \cdots x_{j-1} 1$  until  $n$  numbers are produced.
  - i) If  $n = tj$  for some integer  $t$  then let  

$$Y = x_1 \cdots x_{j-1} 1 x_1 \cdots x_{j-1} 1 \cdots x_1 \cdots x_{j-1} 1$$
  - ii) If  $n > tj$  then finish with  $x_1 \cdots x_{n-tj}$ ,  
 then let  $Y = x_1 \cdots x_{j-1} 1 \cdots x_1 \cdots x_{j-1} 1 x_1 \cdots x_{n-tj}$ .
4.  $Y$  is a least element iff  $n = tj$
5. Repeat beginning at step 1 until the final least element  $(1)^n$  is reached.

TABLE A.1

2 ALGORITHM FOR  $N = 7$ 

|           | Wt |
|-----------|----|
| 0000000   | 0  |
| 0000001   | 1  |
| 0000010 * |    |
| 0000011   | 2  |
| 0000100 * |    |
| 0000101   | 2  |
| 0000110 * |    |
| 0000111   | 3  |
| 0001000 * |    |
| 0001001   | 2  |
| 0001010 * |    |
| 0001011   | 3  |
| 0001100 * |    |
| 0001101   | 3  |
| 0001110 * |    |
| 0001111   | 4  |
| 0010010 * |    |
| 0010011   | 3  |
| 0010100 * |    |
| 0010101   | 3  |
| 0010110 * |    |
| 0010111   | 4  |
| 0011001 * |    |
| 0011010 * |    |
| 0011011   | 4  |
| 0011100 * |    |
| 0011101   | 4  |
| 0011110 * |    |
| 0011111   | 5  |
| 0101010 * |    |
| 0101011   | 4  |
| 0101101 * |    |
| 0101110 * |    |
| 0101111   | 5  |
| 0110110 * |    |
| 0110111   | 5  |
| 0111011 * |    |
| 0111101 * |    |
| 0111110 * |    |
| 0111111   | 6  |
| 1111111   | 7  |

\* Unacceptable

Table A.1 illustrates the algorithm for  $n=7$ . Arranging in order by weight, the least element for each pure cycle is tabulated in Table A.2.

TABLE A.2  
PURE CYCLE LEAST ELEMENTS ( $n=7$ )

|   |         |     |
|---|---------|-----|
| 0 | 0000000 | 0   |
| 1 | 0000001 | 1   |
| 2 | 0000011 | 3   |
|   | 0000101 | 5   |
|   | 0001001 | 9   |
| 3 | 0000111 | 7   |
|   | 0001011 | 11  |
|   | 0001101 | 13  |
|   | 0010011 | 19  |
|   | 0010101 | 21  |
| 4 | 0001111 | 15  |
|   | 0010111 | 23  |
|   | 0011011 | 27  |
|   | 0011101 | 29  |
|   | 0101011 | 43  |
| 5 | 0011111 | 31  |
|   | 0101111 | 47  |
|   | 0110111 | 55  |
| 6 | 0111111 | 63  |
| 7 | 1111111 | 127 |

## LIST OF REFERENCES

1. Chan, A. H., Games, R.A., and Key, E.L., "On the Complexities of de Bruijn Sequences", Journal of Combinatorial Theory, Series A, Vol. 35, pp. 233-246, November 1982.
2. Birkoff, G. and Bartee, T.C., Modern Applied Algebra, McGraw-Hill, 1970.
3. Golomb, S., Digital Communications with Space Applications, Prentice-Hall, 1964.
4. Hall, M. Jr., Combinatorial Theory, Blaisdell, 1967.
5. Fredricksen, H. M., "A Survey of Full Length Nonlinear Shift Register Cycle Algorithms", SIAM Review, Vol. 24, pp. 195-221, April 1982.
6. Technion Report 268, On the Distribution of de Bruijn Sequences of Given Complexity, by T. Etizon and A. Lempel, February 1983.
7. Golomb, S., Shift Register Sequences, Holden-Day, 1967.
8. IEEE Proceedings International Information Theory Conference, 1982, On the Complexity of Functions of Linear Shift Register Sequences, by T. Herlestam, p. 166.
9. Games, R.A. and Chan, A.H., "A Fast Algorithm for Determining the Complexity of a Binary Sequence with a Period  $2^n$ ", IEEE Trans. on Inform. Theory, January 1983.
10. Fredricksen, H.M. and Maiorana, J., "Necklaces of Beads in k Colors and k-ary de Bruijn Sequences", Discrete Math., Vol. 23, No. 3, September 1978.

# INITIAL DISTRIBUTION LIST

|                                                                                                                           | No. Copies |
|---------------------------------------------------------------------------------------------------------------------------|------------|
| 1. Defense Technical Information Center<br>Cameron Station<br>Alexandria, Virginia 22314                                  | 2          |
| 2. Library, Code 0142<br>Naval Postgraduate School<br>Monterey, California 93940                                          | 2          |
| 3. Department Chairman, Code 53Wm<br>Department of Mathematics<br>Naval Postgraduate School<br>Monterey, California 93940 | 1          |
| 4. Prof. Fredricksen, Code 53Fs<br>Department of Mathematics<br>Naval Postgraduate School<br>Monterey, California 93940   | 5          |
| 5. Major Robert L. Holdahl, USMC<br>Department of Mathematics<br>United States Naval Academy<br>Annapolis, Maryland 21402 | 6          |

END

FILMED

6-84

DTIC