TECHNICAL REPORT NO. 165

STUDY OF LINEAR SEQUENCE GENERATORS

by:

C. C. Hoopes
R. N. Randall

Approved by: *[signature]*

T. G. Birdsall

for

COOLEY ELECTRONICS LABORATORY

Department of Electrical Engineering
The University of Michigan
Ann Arbor, Michigan

June 1966

TABLE OF CONTENTS

FOREWORD

This report was prepared by the Cooley Electronics Laboratory, The University

of Michigan, Ann Arbor, on Contract No. DA-28-043 AMC-00080(E). The work was

administered under the direction of the U.S. Army Electronics Materiel Agency, Fort

Monmouth, New Jersey. This report completes one phase of the work performed on

this contract during the period 1 May 1964 to 31 August 1965.

Messrs. Joseph H. Davis and John F. Dickson served as the technical

representatives for the U. S. Army Electronics Command. Their assistance and

guidance are gratefully acknowledged.

The chief contributors and their fields of activity were: T. G. Birdsall, technical

director; C. C. Hoopes, supervisor; R. N. Randall, analysis and experimental

implementation.

The JHG generator was originated by T. G. Birdsall.

LIST OF ILLUSTRATIONS

$E_i(k)$ content vector of a generator after k shifts when the initial content was $E_i(0)$

e_j j-th element of the column vector $E_i(0)$

F_A feedback matrix, n x n matrix derived from the feedback equation of an SSRG or an SCRG

F_M feedback matrix, n x n matrix derived from the feedback equation of an MSRG or an MCRG

$f_{i,j}$ element of matrix F_A

$f(\xi)$ characteristic polynomial of the A matrix associated with a linear sequence generator

$f'(\xi)$
$f''(\xi)$ } factors of $f(\xi)$

$f_i(\xi)$ characteristic polynomial associated with the i stage JHG composed of the first i stages of a given n stage JHG

G   an n x n matrix which commutes between the output sequences produced by adjacent stages of an SCRG for which $c_n = 1$

$g_{i,j}$ element of matrix G

$g(\xi)$ characteristic polynomial associated with the G matrix

H   an n x n matrix which commutes between the output sequences produced by adjacent stages of an SCRG

$h_{i,j}$ element of the matrix H

$h(\xi)$ characteristic polynomial associated with the H matrix

I   identity matrix

I^* the 90° rotation of the identity matrix

$i, j, k, m, n, p, q, r, s, \nu$ integers, index, used to denote stages of a generator, feedback taps, number of shift pulses

$i^*_{j,k}$ elements of the matrix I^*

$J_{i,k}$ time shifts between the sequences produced by the i-th and k-th stages of a maximal generator

JHG   Jacobian-hybrid generator

K   time shift between the sequences produced by adjacent stages of an SCRG, or between adjacent stages of an MCRG which are not separated by an adder, time index

L   number of digits in a maximal length sequence, $L = 2^n - 1$

ℓ length of a sequence, usually reserved for the length of the impulse response sequence of a nonmaximal generator

MCRG	modular-complement-register generator
MSRG	modular-shift-register generator
m	number of different nonmaximal sequences which can be produced by a particular nonmaximal generator
n	integer, number of stages in a linear sequence generator

P_i $n \times n$ matrix, the inverse of the $n \times n$ matrix

$$\begin{bmatrix} E_i(0)^T \\ \vdots \\ E_i(n-1)^T \end{bmatrix}$$

when such an inverse exists.

p, p_i	length of a sequence, usually one of several nonmaximal sequences which can be generated by a given nonmaximal generator
$P_{i,j}$	element of matrix which is the product of $R_2 \cdot F_A$; elements of matrix R_3^{-1}; element of matrix $(I^*)^T$
$q_{j,k}$	element of matrix $(I^*)^2$
R_i	a square matrix (usually $n \times n$) composed of the mod-2 binomial coefficients $(i = 1, 2, 3, 4)$
$r^i_{j,k}$	element of matrix R_i $(i = 1, 2, 3, 4)$
SCRG	simple-complement-register generator
SRG	shift-register generator
SSRG	simple-shift-register generator
$s_{i,j}$	element of matrix R_4^{-1}
T	symbol used to denote the transpose of a matrix A^T = transpose of A
$t_{i,j}$	element of matrix which is the product of $H \cdot G$
U' U"	transient content vectors
U(j)	content vector of generator at time j
$u_i(j)$	content of the i-th stage of a generator at time j
$V_i(j)$	an $n \times 1$ column vector of consecutive digits produced by the i-th stage of a generator; an n-tuple of digits from sequence $x_i(j)$
$V'_i(j)$	an $(n-k) \times 1$ column vector consisting of the elements $u_i(j+k), \ldots, u_i(j+n-1)$
X(j)	$1 \times n$ row vector made up of the first n digits of output from a grand mod-2 adder; a linear binary sequence

$X_i(j)$ — linear binary sequence produced by the i-th stage of a linear-sequence generator, with time reference j; any indexed sequence

x — general indeterminant

x_i — element of row vector $X(j)$, $x_i = x(i-1)$

$x(j)$ — digit of sequence $X(j)$; output digit from grand mod-2 adder at time j

$x_i(j)$ — element of $X_i(j)$

$Y(j)$ — content vector of an SSRG at time j

$y_i(j)$ — content of the i-th stage of an SSRG at time j

$\overline{\alpha}$ — 1 x n row vector representing the tap connections for a grand mod-2 adder

α_i — binary digit corresponding to the i-th switch connection for a grand mod-2 adder

$\delta_{i,j}$ — Kronecker delta $\delta_{i,j} = 1$ when $i = j$, $\delta_{i,j} = 0$ otherwise

ξ — general indeterminant

τ — an operator which operates on a sequence $X_i(j)$ and performs the function of shifting that sequence ahead one digit

ψ — general indeterminant

$\binom{k}{i}$ — coefficient in the binomial expansion $(x+1)^k = \sum\limits_{i=0}^{k} \binom{k}{i} x^i$

LIST OF APPENDICES

ABSTRACT

This report treats techniques for generating linear binary sequences. The basic properties of sequence generators, maximal sequences, and non maximal sequences are reviewed. Five specific types of generators, each representing a "canonical form," are considered. Two forms of shift-register generators are studied: the simple-shift-register generator and the modular-shift-register generator. Two forms of complement-register generators are considered: the simple-complement-register generator and the modular-complement-register generator. A hybrid generator consisting of both shift and complement stages is discussed. Included in the discussion for each generator are: (1) the relationship between the characteristic polynomial and the feedback connections, (2) the relationship between sequences produced by different stages of the same generator, (3) the initial loading required for the generator to produce a particular n-tuple from the output stage, and (4) an output adder technique to obtain the desired starting conditions for a sequence obeying the law of the generator.

The advantages and disadvantages of each of the five generators are given. Also tables of equivalent generators for all maximal characteristic polynomials of degree $2 \leq n \leq 12$ are included.

Matrix theory is used throughout the report to prove necessary theorems, and it is used in the development of mathematical descriptions of the generators. Short proofs and derivations are presented in the text; more complex proofs and derivations are usually reserved for the appendices.

1. INTRODUCTION

In recent years the application of digital sequences in communications, radar, and guidance systems has increased. Considerable attention in the literature has been given to the properties and characteristics of digital sequences. This report considers techniques for generating periodic, deterministic, linear, binary sequences (only linear techniques will be treated). The binary states, for convenience in this report, will consist of 0's and 1's.

One common technique, used extensively in the past for generating binary sequences, is the shift-register generator which essentially consists of a basic shift register to which modulo-two adders have been added. These adders are connected to various stages of the register. The outputs from the register stages form the inputs to the modulo-two adders, and outputs of the adders are fed back to some other stage of the register so that one or more closed loops are formed. When the shift register is then pulsed in the normal manner, the output from any stage of the register forms a digital sequence. In the general case, depending upon both the feedback connections and upon the initial loading of the shift register, the ensuring digital sequence has a period much longer than the number of stages in the register.

Digital sequences can also be generated using a "complement register" around which some form of modulo-two adder feedback loop is employed rather than by using a shift register. The "complement register" consists of a cascading of complement stages (a ONE input causes the stage contents to change) rather than the cascading of shift stages (the input is stored directly) found in the shift-register. Combinations of complement and shift stages can also be employed to form "hybrid" generators.

This report presents in one volume a basic treatment of linear generation techniques, and discusses some of the more important properties and advantages of the different types of generators. No attempt will be made here to treat the application of such sequences to practical systems.

In Section 2, the basic properties of linear sequence generators and linear sequences are reviewed to introduce the terminology and notation to be used throughout the report.

In Sections 3 and 4, we review the properties of the simple-shift-register generator (SSRG) and of the modular-shift-register generator (MSRG). These types of generators have been treated extensively in earlier reports (see Refs. 1,2), but are included in this report for completeness.

The theory of the simple-complement-register generator (SCRG) and the modular-complement-register generator (MCRG) is developed in Sections 5 and 6 in a manner similar to the discussion of shift-register generators.

Section 7 presents an introduction to the "Jacobian-hybrid generator" (JHG) which is a form of hybrid generator that employs both complement and shift stages.

Section 8 concludes the report with a comparison of the properties, and of the advantages and disadvantages of the different types of generators we have discussed.

The notation used in this report follows that of Refs. 1 and 2. The properties and theorems developed in these references are often duplicated in this report without proof.

2. GENERAL PROPERTIES

In this section the basic properties of linear sequences and of linear generators are reviewed. These properties are generally true, regardless of the type of linear generator being discussed. Basic definitions and notations are also developed to use in the remainder of this report.

2.1 The A Matrix

The A matrix, which we define below, performs this function: if one multiplies on the left the n-row column content vector, which represents the n contents of an n stage generator, by this matrix, then one obtains the contents of the generator after one shift. This matrix is equivalent in function to running the generator one step at a time.

Let $u_i(j)$ be the content of the i-th stage of the generator at time j. The content vector U(j) is the n x 1 column vector

$$U(j) \quad = \quad \begin{bmatrix} u_1(j) \\ u_2(j) \\ \vdots \\ u_n(j) \end{bmatrix} \tag{1}$$

where $u_i(j)$ = 1 or 0 depending upon the binary content of the i-th stage at time j. The content vector one shift later, U(j + 1), becomes

$$U(j + 1) \; = \; A \; U(j) \qquad (\text{mod-}2) \tag{2}$$

or, for any number of shifts k

$$U(j + k) \; = \; A^k \; U(j) \qquad (\text{mod-}2) \tag{3}$$

The n x n matrix A is defined as

$$A \; = \; \begin{bmatrix} a_{i,j} \end{bmatrix}_{nxn}$$

where

$\quad a_{i,j}$ = 1 if stage j feeds stage i

$\qquad\quad$ = 0 if stage j does not feed stage i. $\tag{4}$

3

For example, the A matrix, using Eq. 4, for the _multiple return_ shift-register generator in Fig. 1 is

$$A \ = \ \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{5}$$
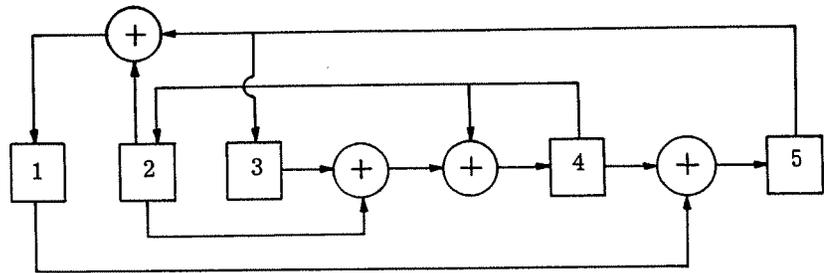
Fig. 1. A five-stage multiple return shift-register generator.[1]

---

[1] $\oplus$ denotes modulo-2 addition. A "mod-2 adder," or "exclusive or" circuit produces a "ONE" output if, and only if, the inputs are different.

$\boxed{i}$ denotes a shift register stage. In Section 5, complement register generators are considered for which each stage is a complement stage and denoted as $\boxed{i_c}$.

2.2 Characteristic Polynomial and Sequence Law

Let $f(\xi)$ be the _characteristic polynomial_ of the A matrix for a given generator. By definition, the characteristic polynomial is the determinate $|A - \xi I|$. Since (-1) and (+1) are the same in modulo-2 arithmetic,

$$f(\xi) \ = \ |A + \xi I| \ . \qquad (\text{mod-}2) \tag{6}$$

Further, let b_i represent the coefficients of this nth degree polynomial $f(\xi)$, that is

$$f(\xi) \ = \ \sum_{i=0}^{n} b_i \, \xi^{i} \qquad (\text{mod-}2) \tag{7}$$

where b_n is always one, and the other b_i coefficients are either zero or one.

Associated with every characteristic polynomial $f(\xi)$ is the "companion matrix," C_f,

4

$$C_f = \text{companion matrix} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ & \vdots & & & & \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ b_0 & b_1 & b_2 & \cdots & b_{n-2} & b_{n-1} \end{bmatrix} \tag{8}$$

Note that the companion matrix is nonsingular whenever $b_0 \equiv 1$; this can be seen by expanding the determinate, $|C_f|$, by minors by the first column

$$|C_f| \equiv b_0 \tag{9}$$

The characteristic equation is defined as

$$f(\xi) = 0$$

that is,

$$\sum_{i=0}^{n} b_i \xi^i = 0 \qquad (\text{mod-}2) \tag{10}$$

By the Hamilton-Cayley Theorem (see Ref. 3), a matrix satisfies its own characteristic equation, thus

$$f(A) = \sum_{i=0}^{n} b_i A^i = 0 \qquad (\text{mod-}2) \tag{11}$$

Using Eqs. 3 and 11:

$$f(A) \, U(j) = \sum_{i=0}^{n} b_i A^i \, U(j) = 0 \quad (\text{mod-}2)$$

$$= \sum_{i=0}^{n} b_i \, U(j+i) = 0 \quad (\text{mod-}2) \tag{12}$$

By changing the time index and because (+1) equals (-1) for mod-2 addition, Eq. 12 can be rewritten as

$$b_n \, U(j) = U(j) = \sum_{i=1}^{n} b_{n-i} \, U(j-i) \qquad (\text{mod-}2) \tag{13}$$

The characteristic sequence law is derived from Eq. 13

$$u_k(j) = \sum_{i=1}^{n} b_{n-i} \, u_k(j-i) \qquad (\text{mod-}2) \tag{14}$$

for $k = 1, 2, \ldots, n$.

The characteristic sequence law relates the present contents of any stage of a generator to the previous n contents of the same stage. Notice that the sequences produced by each stage of the generator obey the characteristic sequence law for the generator.

Let the column vector $V_i(j)$ represent an n-tuple of successive bits from the ith stage of a linear generator starting at time j, that is

$$V_i(j) = \begin{bmatrix} u_i(j) \\ u_i(j+1) \\ \vdots \\ u_i(j+n-1) \end{bmatrix} \tag{15}$$

The companion matrix, C_f, corresponding to the characteristic polynomial, $f(\xi)$, for the generator can be used to find $V_i(j+k)$ by

$$V_i(j+k) = C_f^k V_i(j) \qquad (\text{mod-2}) \tag{16}$$

where

$$V_i(j+k) = \begin{bmatrix} u_i(j+k) \\ u_i(j+k+1) \\ \vdots \\ u_i(j+k+n-1) \end{bmatrix}$$

and C_f is as defined in Eq. 8.

To verify Eq. 16, consider the product

$$C_f V_i(j) \qquad (\text{mod-2}) \tag{17}$$

The first n-1 rows of product in Eq. 17 are $u_i(j+1)$, $u_i(j+2), \ldots, u_i(j+n-1)$, respectively. The nth row of the product is

$$b_0 u_i(j) + b_1 u_i(j+1) + \ldots + b_{n-1} u_i(j+n-1), \quad (\text{mod-2}) \tag{18}$$

From Eq. 14, the characteristic sequence law, the sum in Eq. 18 reduces to $u_i(j+n)$. The product in Eq. 17 is, therefore,

$$V_i(j+1) = C_f V_i(j) \qquad (\text{mod-2}) \tag{19}$$

6

Equation 16 readily follows from Eq. 19 by repeated application of Eq. 19.

Let $X(j) = x(j), x(j+1), x(j+2), \ldots$, represent a sequence with time reference j. The individual digits of $X(j)$, $x(j+k)$, are the successive outputs from some stage of a sequence generator. The mod-2 sum of two sequences $X_1(j) + X_2(j)$ by definition becomes

$$X_1(j) + X_2(j) = x_1(j) + x_2(j),\ x_1(j+1) + x_2(j+1),\ \ldots \quad \text{(mod-2)} \tag{20}$$

Theorem 1:

If $X_1(j)$, $X_2(j)$, $\ldots$, $X_m(j)$ are sequences, all of which have the same characteristic sequence law, $\sum_{i=0}^{n} b_{n-i}\, x_k(j-i) = 0 \ \text{(mod-2)}$, then their sum

$$X(j) = \sum_{i=1}^{m} X_i(j) \quad \text{(mod-2)}$$

also obeys the same characteristic sequence law.

Proof:

For $k = 1, 2, \ldots, m$, the individual digits of $X_k(j)$ are determined by the sequence law

$$x_k(j+s) = \sum_{i=1}^{n} b_{n-i}\, x_k(j+s-i) \quad \text{(mod-2)}$$

$$s = 0, \pm 1, \pm 2, \ldots \tag{21}$$

The sum sequence $X(j)$ is composed of $x(j+s)$, where

$$x(j+s) = \sum_{k=1}^{m} x_k(j+s) \quad \text{(mod-2)}, \quad s = 0, \pm 1, \pm 2, \ldots$$

$$= \sum_{k=1}^{m} \sum_{i=1}^{n} b_{n-i}\, x_k(j+s-i) \quad \text{(mod-2)}$$

$$= \sum_{i=1}^{n} b_{n-i} \sum_{k=1}^{m} x_k(j+s-i) \quad \text{(mod-2)}$$

$$= \sum_{i=1}^{n} b_{n-i}\ x(j+s-i) \quad \text{(mod-2)} \tag{22}$$

Comparing Eqs. 21 and 22 we can see that the sum sequence $X(j)$ obeys the same sequence law that $X_1(j)$, $X_2(j)$, $\ldots$, $X_m(j)$ obey.

7

In the remainder of this report the following notational convention will be used for the characteristic polynomial:

$$(n, a, \ldots, b) \text{ means } f(\xi) = \xi^n + \xi^a + \ldots + \xi^b \quad (\text{mod-2}) \tag{23}$$

For example, from Eqs. 5, 6, and 23 the characteristic polynomial for the generator in Fig. 1 is the determinate

$$f(\xi) = |A + \xi I| = \begin{bmatrix} \xi & 1 & 0 & 0 & 1 \\ 0 & \xi & 0 & 1 & 0 \\ 0 & 0 & \xi & 0 & 1 \\ 0 & 1 & 1 & 1+\xi & 0 \\ 1 & 0 & 0 & 1 & \xi \end{bmatrix} = \xi^5 + \xi^4 + \xi + 1 = (5, 4, 1, 0) \quad (\text{mod-2})$$

2.3 Maximal Sequences and Generators

Under certain conditions, sequence generators produce sequences that begin with a number of binary digits which are not part of the periodic portion of the sequence. These bits which are not a part of the periodic sequence will be referred to as transient bits. (Transient bits are discussed further in Section 2.4.2.)

Given any n consecutive bits of a periodic sequence from an n-stage generator, the entire periodic sequence is uniquely determined by application of the characteristic sequence law. As a result, any given n-tuple of consecutive bits of a sequence can appear in only one periodic sequence produced by the generator. For a transient free generator, every possible n-tuple will appear in one and only one of the periodic sequences. It should be noted that to obtain all of the periodic sequences produced by a generator various initial conditions may be required.

Consider an n-tuple of consecutive binary digits (bits) of a sequence $\{x(j), x(j+1), \ldots, x(j + n - 1)\}$. There are 2^n possible binary n-tuples. One of these, however, is all 0's. If $x(j + i) = 0$ for $i = 0, 1, \ldots, n-1$, then from the characteristic sequence law

$$x(j+n) = \sum_{i=1}^{n} b_{n-i} \, x(j+n-i) = 0 \quad (\text{mod-2})$$

and every following bit will also be zero. Consequently, the all zero n-tuple will appear only in the all-zero sequence (null sequence) with a period of one bit. This particular sequence

will not be considered in the remaining portions of this report. There remain $2^n - 1$ nonzero n-tuples which can appear in a sequence or sequences from a generator. Consequently, the maximum number of digits in a periodic sequence generated by an n-stage linear generator is $2^n - 1$ before the sequence begins to repeat itself. Therefore, any sequence of length

$$L \equiv 2^n - 1 \tag{24}$$

will be defined as a maximal sequence if every n-tuple except the all zero n-tuple appear in it.

An important property of maximal sequences is the shift-and-add property: if a maximal sequence is shifted in time and added to itself, then the resulting sequence will be the same maximal sequence shifted in time, or all zeros. That is, if X(j) is a maximal sequence, then

$$X(j) + X(j + k) = X(j + r) \quad (\text{mod-}2) \tag{25}$$

where k and r are non zero integer constants mod- $L = 2^n - 1$. The shift-and-add property follows from (1) Theorem 1; (2) the fact that any n-tuple and the sequence law completely determines the sequence; and, (3) the fact that a maximal sequence contains every non zero n-tuple of binary digits.

Another property of maximal sequence generators is:

Theorem 2:

Every stage of a maximal sequence generator produces the same sequence, but the sequence (except for the null sequence) from any stage will be shifted in time from the sequence produced by any other stage.

The proof of this theorem appears in Appendix A.

2.4 Nonmaximal Sequences and Generators

Since any sequence of length $L \equiv 2^n - 1$, where n is the number of stages in the generator, has been termed a maximal sequence, any sequence of length $p < L = 2^{n-1}$ will be termed a nonmaximal sequence. Furthermore, if a transient free n-stage generator produces m different nonzero periodic sequences (obtained by using different initial loadings in the generator) with periods, $p_1, p_2, \ldots, p_m$, then

$$\sum_{i=1}^{m} p_i = 2^n - 1 = L \tag{26}$$

9

Non maximal sequences can be separated into two categories: (1) those associated with irreducible characteristic polynomials and, (2) those associated with factorable characteristic polynomials.

2.4.1 Irreducible Characteristic Polynomials. If the characteristic polynomial associated with a non maximal sequence law is irreducible, it has been found (see Ref. 1) that there are m sequences of the same length, ℓ , which obey that sequence law, and by Eq. 26

$$m\ell = L \tag{27}$$

where ℓ is called the impulse response length.[2] Non maximal sequences corresponding to irreducible characteristic polynomials exhibit a partial shift-and-add property. That is, for certain shifts the mod-2 sum will give back the same non maximal sequence and the shift-and-add property holds.[3]

2.4.2 Factorable Characteristic Polynomials. It has been shown in Ref. 1 that if the characteristic polynomial, $f(\xi)$, of a generator is factorable such that

$$f(\xi) = f'(\xi) \cdot f''(\xi) \ldots f'''(\xi) \quad (\text{mod-}2)$$

then the generator is non maximal. Further, the sequences that obey the sequence laws associated with the factors of the characteristic polynomial are among the sequences that obey the sequence law of the generator.

For example, if the characteristic polynomial for a five -stage generator is

$$(5, 4, 0) = (2, 1, 0)(3, 1, 0) \quad (\text{mod-}2) \tag{28}$$

then the generator is non maximal. The sequences associated with a (2, 1, 0) characteristic polynomial and the (3, 1,0) characteristic polynomial are among the sequences associated with a (5, 4, 0) characteristic polynomial.

This property suggests a useful physical representation of a non maximal generator with a characteristic polynomial that is factorable (Ref. 1). This representation consists of

---

[2] The impulse response length, ℓ, is defined for any transient free generator as the length of that periodic sequence (produced by that generator) which contains n-1 successive "zeros" preceded and followed by a "one".

[3] For a more complete discussion, see Ref. 1.

10

a consideration of each factor as representing a separate generator, and a cascading of the resulting generators, as the factors themselves are cascaded in the equation. Figure 2a illustrates this representation of a generator with a polynomial that is factorable. Each generator in the cascaded group has its feedback connnections constructed according to the terms in the corresponding factor. The object of this representation is to be able to view the generation of the entire set of sequences from the total generator as stemming from different combinations of factor generator sequences. In this process, the indivdual generators are allowed to take on all their possible sequences, including the all-zero sequence. This representation has been shown to be always valid. It also serves as a useful means for considering the set of sequences from a factorable non maximal generator.

$$\text{polynomial} = (n,j,\dots) = (k,m,\dots)(p,r,\dots)(s,t,\dots)$$

(a)

$$(n,j,\dots) = (k,m,\dots)(p,r,\dots)(s,t,\dots)$$

(b)
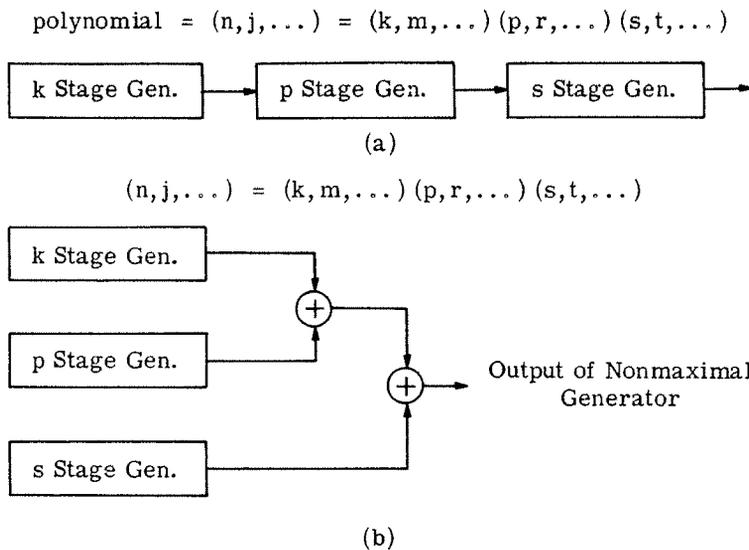
Fig. 2. (a) Physical interpretation of a generator whose polynomial
is factorable, (b) concept of "beating" the factor generators
when the factors are nonrepeating.

In addition to the interpretation of Fig. 2a, another physical interpretation can be given for non repeated factors (Ref. 1). This interpretation views the sequences from the factors as "beating" to form the sequences of the total generator (whereas, the conception of Fig. 2a considers the factors as cascaded generators). "Beating" means operating the factor generators independently, and mod-2 adding the outputs. The word "beating" comes from the frequency spectrum analysis of the result, which contains the sum and difference of "the beats" of the individual sequence spectral lines. For a general polynomial, this

11

concept is depicted in Fig. 2b. This beating concept applies only when the factors of the polynomial are non repeating. It does not work when there are repeated factors.

There are two particular types of factorable characteristic polynomials which rate special mention. The first is the characteristic polynomial that has $(\xi + 1)$ as a factor.

Theorem 3:

The term $(\xi + 1)$ is a factor of the characteristic polynomial

$$f(\xi) = \sum_{i=0}^{n} b_i \, \xi^i \quad (b_n = 1) \quad (\text{mod-2})$$

if, and only if,

$$\sum_{i=0}^{n} b_i = 0 \quad (\text{mod-2})$$

That is, there is an even number of terms in $f(\xi)$. This theorem is proved in Ref. 1, p. 104.

An immediate consequence of Theorem 3 is that the characteristic polynomial for a maximal sequence generator has an odd number of terms.

The second factorable characteristic polynomial that is a special case of interest is one which has ξ^k as a factor.

Theorem 4:

Let the characteristic polynomial $f(\xi)$ have the form

$$f(\xi) = \xi^k \sum_{i=k}^{n} b_i \xi^{i-k} \quad (\text{mod-2})$$

where $b_n = b_k = 1$

then

(1) the sequence obtained from any stage of the generator may begin with a transient of k or fewer bits (not part of the periodic sequence), after which the sequence becomes periodic and obeys the sequence law of an n-k stage generator with characteristic polynomial

$$f'(\xi) = \sum_{i=k}^{n} b_i \xi^{i-k} \quad (\text{mod-2})$$

12

(Note: the sequence may start out with up to k transient bits and then produce the null sequence.)

(2) There is at least one non zero content vector, U', so that if the generator is initially loaded with U', there will be one transient content vector before every stage produces the null sequence.

(3) If the generator is capable of producing any non zero periodic sequence, $(k < n)$, then there is at least one non zero content vector, U'', so if the generator is initially loaded with U'' there will be exactly one transient content vector before the generator output becomes periodic and at least one stage produces a non zero sequence.

The proof of Theorem 4 is found in Appendix A. The most important consequences of Theorem 4, for the purpose of this report, are (1) that a generator is transient free, if and only if, $b_o \equiv 1$, and (2) any periodic sequence that can be produced by a generator with a characteristic polynomial that has ξ^k as a factor (i. e. , $b_i = 0$, $0 \leq i < k$), can be produced by a generator of n - k stages. For these reasons the remainder of this report will deal primarily with generators having characteristic polynomials with a nonzero constant term ($b_o \equiv 1$).

2. 5 The B_A Matrix

The B_A matrix is a matrix associated with the A matrix of a sequence generator and is derived by using the characteristic equation of the A matrix.

Each power of A can be expressed in terms of powers of A no larger than n-1 (where n is the number of stages in the generator). The B_A matrix represents a "table" of these expressions. The B_A matrix is defined by the equation

$$B_A = [b_{i,j}] \tag{29}$$

where the elements $b_{i,j}$ are the coefficients in the equation

$$A^i = \sum_{j=1}^{n} b_{i,j} A^{n-j} \quad (\text{mod-} 2) \tag{30}$$

The coefficients $b_{i,j}$ will form either an L by n or an ℓ by n matrix. The B_A matrix is essentially constructed by successively raising the powers in an equation, starting with

the identity $A = A$, and ending with $A^{\ell} = I$ or $A^L = I$. Whenever the power of n appears on the right hand side, it is replaced by use of the characteristic equation.

For example, given a generator with a characteristic polynomial of (4, 2, 0) or equivalently $A^4 = A^2 + I$, the B_A matrix is derived as follows:

$$A = A$$

$$A^2 = A^2 \qquad \text{(mod-2)}$$

$$A^3 = A^3 \qquad \text{(mod-2)}$$

$$A^4 = A^2 + I \qquad \text{(mod-2)}$$

$$A^5 = A \cdot A^4 = A^3 + A \qquad \text{(mod-2)}$$

$$A^6 = A \cdot A^5 = A^4 + A^2 = A^2 + I + A^2 = I \qquad \text{(mod-2)}$$

and the B_A matrix becomes

$$
\text{powers of } A \longrightarrow \quad 3 \quad 2 \quad 1 \quad 0
$$

$$
B_A = \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array}
\begin{bmatrix}
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
$$

For any non singular (transient free) A matrix ($b_0 = 1$) the last row of the B_A matrix will be n-1 "zeros" followed by a "one", like the above example. This row then represents the <u>smallest</u> power ℓ so that [4]

$$A^{\ell} = I \quad \text{(mod-2)} \tag{31}$$

Every sequence produced by that generator will be periodic every ℓ bits. Therefore, if the nonmaximal generator produces any sequences of length $p < \ell$, then ℓ must be some integral multiple of p. A formal proof of this can be found in Ref. 1, p. 95.

The B_A matrix is obtained by application of the characteristic polynomial of the A matrix. Thus, two different A matrices with identical characteristic polynomials have identical B_A matrices.

---

[4]The impulse response length ℓ is defined in Section 2. 4. 1.

.6 Equivalence of Two Linear Sequence Generators

Two linear sequence generators are said to be <u>equivalent</u> if every sequence produced y one can be produced by the other, and vice versa.

Since the sequences produced by a generator depend entirely upon the characteristic equence law, necessary and sufficient conditions for equivalence are:

(1) The linear sequence generators must have the same characteristic polynomials;

(2) For every n-tuple of consecutive bits of a sequence obtainable from one generator, there exists an initial loading for the other generator which will generate the required n-tuple at the selected output stage of the generator.

The properties and relationships developed in this sectioon are vaild for any linear sequence generator. In the following section, specific types of linear generators are considered and some of the more important properties of each type of generator are discussed.

3. THE SIMPLE SHIFT-REGISTER GENERATOR

A linear shift-register generator (SRG) is any device using a binary memory register, that produces an output binary sequence when successively triggered by a "shift" command. A linear generator means that the changes in the register contents are those of a time-invariant linear operator. The shift register may include sets of storage units in which a particular content does not necessarily move to an adjacent position, but may move to various other positions depending upon the connections between the units (see Fig. 1). To form a shift-register generator, modulo-two adders are attached to a basic memory register to form feedback and/or feedforward loops.

In this section, one standard form of shift-register generator (SRG) is considered, namely the "simple-shift-register generator" (SSRG). The SSRG is defined; and, the A matrix, characteristic polynomial, and characteristic sequence law for it are discussed.

The treatment given to the SSRG in this section and that given to the "modular-shift register," in the next section, are included in this report only for the sake of completeness. More detailed discussions of these two types of SRG's are given in Refs. 1 and 2.

3.1 Definition

In a simple shift register, each stage is fed by its immediate predecessor. In an SSRG, the contents of certain stages are added (mod-two) to feed the first stage. The switches, denoted as c_i, represent the "feedback taps" of the SSRG in Fig. 3a.

$$c_i = 1 \text{ if the ith stage of the SSRG feeds the 1st stage}$$

$$= 0 \text{ if the ith stage of the SSRG does not feed the 1st stage} \tag{32}$$

By convention $c_0 \equiv 1$, and normally $c_n = 1$. (See p. 20 where $c_n \neq 1$.)

In the SSRG there are only feedback loops to the first stage. No interstage adders are present. If the sequences themselves were the only item of interest there would be no loss in generality by considering only this type of SRG. Every linear generator can

be shown to have an equivalent SSRG, (Section 3. 4).

The block diagram of Fig. 3b will be used to represent an SSRG without showing interstage connections as in Fig. 3a.
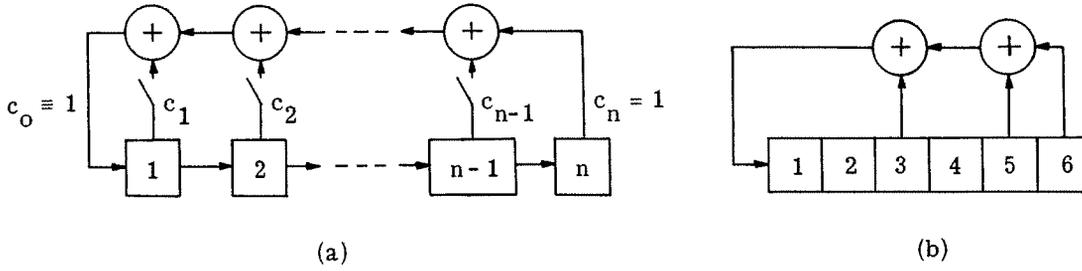
Fig. 3.   (a) An n-stage simple shift-register generator,
(b) a six-stage SSRG with feedback taps
c_5 and c_3 closed.

3.2   The A Matrix

From Section 2. 1, the A matrix is defined by the following relation:

$$A = [a_{i,j}]$$

where

$a_{i,j}$ = 1 if the jth stage of the SRG feeds into the ith stage of the SRG

= 0 otherwise.

From Fig. 3 it is obvious that the content of the ith stage of the SSRG at time j, $u_i(j)$, is given by the relationships:

$$\left. \begin{array}{l} u_1(j) = \displaystyle\sum_{k=1}^{n} c_k\, u_k(j-1) \qquad (\text{mod-}2) \\[2em] u_i(j) = u_{i-1}(j-1), \qquad 2 \le i \le n \end{array} \right\} \tag{33}$$

For the SSRG with feedback taps c_j , the A matrix becomes

$$A = [a_{i,j}]$$

where

$$
\left.
\begin{aligned}
a_{1,j} &= c_j , && j = 1,2,\ldots,n \\[2mm]
a_{i,i-1} &= 1 , && i > 1 \\[2mm]
a_{i,j} &= 0 && \text{otherwise}
\end{aligned}
\right\}
\qquad (34)
$$

$$
A =
\begin{bmatrix}
c_1 & c_2 & c_3 & \cdots & c_{n-1} & c_n \\
1 & 0 & 0 & \cdots & 0 & 0 \\
0 & 1 & 0 & \cdots & 0 & 0 \\
& & \vdots & & \vdots & \\
0 & 0 & 0 & \cdots & 0 & 0 \\
0 & 0 & 0 & \cdots & 1 & 0
\end{bmatrix}
\qquad (35)
$$

3.3 Characteristic Polynomial, Sequence Law, and Feedback Equation

The characteristic polynomial for the SSRG, from Eq. 7, is defined as

$$f(\xi) = |A + \xi I| = \sum_{i=0}^{n} b_i \xi^i \qquad (\text{mod-2})$$

where $b_n \equiv 1.$

If the A matrix of Eq. 35 is rotated 180°, one obtains

$$
A^R = A \text{ rotated } 180^{\circ} =
\begin{bmatrix}
0 & 1 & 0 & \cdots & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 \\
c_n & c_{n-1} & c_{n-2} & \cdots & c_2 & c_1
\end{bmatrix}
\qquad (36)
$$

18

which by comparing Eq. 8 is the companion matrix for the characteristic polynomial

$$f(\xi) = \xi^n + \sum_{j=1}^{n} c_j \, \xi^{n-j}$$

By defining $c_0 \equiv 1$, the characteristic polynomial for an SSRG is

$$f(\xi) = |A + \xi I|$$

$$= \sum_{j=0}^{n} c_j \, \xi^{n-j} \qquad (\text{mod-}2) \qquad (37)$$

where

c_j are the feedback taps of the SSRG

$c_0 \equiv 1$

$c_j = 1$ if the jth stage is in the feedback loops

    $= 0$ otherwise

By comparing Eqs. 7 and 37, the characteristic polynomial for the SSRG is determined by the relationship

$$b_i = c_{n-i} \qquad i = 0, 1, 2, \ldots, n \qquad (38)$$

where the b_i's are the coefficients in the characteristic polynomial Eq. 7, and the c_i's are the feedback taps of the SSRG. From Eqs. 14 and 38, the characteristic sequence law for an SSRG becomes

$$u_i(j) = \sum_{k=1}^{n} c_k \, u_i(j-k) \qquad (\text{mod-}2)$$

$$\text{for} \quad i = 1, 2, \ldots, n \qquad (39)$$

A shorthand notation for describing an SSRG is

$$[n, a, \ldots, b, 0]_{ss} : \begin{array}{l} \underline{\text{feedback equation}} \text{ which specifies an} \\ \text{SSRG with feedback taps } n, a, \ldots, b \\ \text{closed.} \end{array} \qquad (40)$$

Note that 0 has been placed in the feedback equation for convenience to indicate that $c_0 \equiv 1$. Also the n-th stage is included in the feedback loop.

From Eqs. 23, 38, and 40 we can see that the characteristic polynomial and the feedback equation for the SSRG are "simple reverses" of each other. That is

characteristic polynomial $\iff$ feedback equation

$$(n, a, b, \ldots, c, 0) \iff [n, n-c, \ldots, n-b, n-a, 0]_{ss} \qquad (41)$$

Example:

The six-stage SSRG in Fig. 3b with feedback taps c_6, c_5, and c_3 closed has the feedback equation and the characteristic polynomial

$$[6, 5, 3, 0]_{ss} \iff (6, 3, 1, 0)$$

The relationship between the feedback taps and the coefficients in the characteristic polynomial point out these two important properties of SSRG's:

(1) Theorem 4 states that any sequence, from a generator with a characteristic polynomial having no constant term ($b_0 = 0$), can be generated by a generator with less than n stages (disregarding transients). Therefore, since $c_n = b_0$, any periodic sequence from an SSRG in which $c_n = 0$ can be generated by a transient free SSRG with fewer than n stages. Such generators will not be considered in this report and the condition $c_n \equiv 1$ will be implied for all n stage SSRG's.

(2) Theorem 3 states that if

$$\sum_{i=0}^{n} b_i = 0 \qquad (\text{mod-2})$$

then, $(\xi + 1)$ is a factor of $f(\xi)$ and the generator is nonmaximal. For the SSRG $b_i = c_{n-i}$, thus,

$$\sum_{i=0}^{n} b_i = \sum_{i=0}^{n} c_{n-i} = \sum_{i=0}^{n} c_i, \qquad (\text{mod-2})$$

20

and if,

$$\sum_{i=0}^{n} c_i = 0 \qquad (\text{mod-}2)$$

then, $(\xi + 1)$ is a factor of $f(\xi)$. Therefore, for a maximal

SSRG,

$$\sum_{i=0}^{n} c_i = 1 \qquad (\text{mod-}2) \tag{42}$$

Every maximal SSRG must have an even number of feedback

taps (not counting $c_0 \equiv 1$). A table of all maximal SSRG's of

length $2 \leq n \leq 12$ is presented in Section 8.3.

3.4 Initial Loading

The initial loading problem is one of determining the initial content vector $U(j)$

for a generator to obtain a desired n-tuple of consecutive bits from the last stage of the

generator. (Since any n consecutive bits of a sequence along with the characteristic sequence

law uniquely determine the sequence, the initial loading problem is equivalent to finding the

initial loading of a generator necessary to obtain a particular sequence from the last stage

starting at a given place in the sequence.)

Let $\{u_n(j), u_n(j+1), \ldots, u_n(j+n-1)\}$ be the desired n-tuple of bits from the last

stage starting at time j. Then from Eq. 33

$$u_i(j) = u_{i+1}(j+1)$$

and by successive application of Eq. 33,

$$u_i(j) = u_n(j+n-i) \tag{43}$$

Equation 43 specifies the necessary initial loading to obtain the desired n-tuple output.

Let the column vector $V_i(j)$ represent n consecutive output bits from the i-th

stage of the SSRG as in Eq. 15, that is

$$V_i(j) = \begin{bmatrix} u_i(j) \\ u_i(j+1) \\ u_i(j+2) \\ \cdot \\ \cdot \\ \cdot \\ u_i(j+n-1) \end{bmatrix}$$

where $u_i(j)$ = contents of the i-th stage of the SSRG at time j.   Let

$$I^* = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & 0 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 & 0 \\ 0 & 0 & 0 & \ldots & 1 & 0 & 0 \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ 0 & 0 & 1 & \ldots & 0 & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 & 0 \end{bmatrix} \tag{44}$$

then the initial tuple loading U(j) for a desired n-tuple output from the last stage, $V_n(j)$, is

found from the relationship

$$U(j) = I^* V_n(j) \tag{45}$$

where

$$U(j) = \begin{bmatrix} u_1(j) \\ u_2(j) \\ \cdot \\ \cdot \\ \cdot \\ u_n(j) \end{bmatrix}$$

For any n-stage linear sequence generator, the characteristic polynomial and sequence law can be found from the A matrix. Given the characteristic sequence law, any n-tuple of consecutive bits completely determines the sequence. From either Eq. 39 or 41, the feedback equation for an SSRG can be found for any sequence law or characteristic polynomial. From either Eq. 43 or 45, the necessary initial loading for the SSRG can be determined to generate a desired n-tuple of consecutive bits as the starting output of the last stage. Hence,

Theorem 5

Any sequence that can be generated by a linear sequence generator can be generated by an SSRG.

Theorem 5 can be restated as follows: Every linear sequence generator has an equivalent SSRG.

3.5 Interstage Relationships

The relationship between the output sequences obtained from the different stages is particularly uncomplicated for a simple shift-register generator. From Eq. 33

$$u_{i+1}(j) = u_i(j-1)$$

or

$$u_{i+k}(j) = u_i(j-k) \tag{46}$$

That is, the contents of the $(i+k)$-th stage are the same as the contents of the i-th stage k shifts earlier. Thus, if $X_i(j)$ denotes the output sequence produced at the i-th stage, then from Eq. 46

$$X_{i+k}(j) = X_i(j-k) \tag{47}$$

or equivalently, for periodic sequences

$$X_i(j) = X_{i+k}(j+k) \tag{48}$$

3.6 Output Adder Circuit

As contrasted with the direct technique of loading the generator with the proper initial conditions (Section 3.4), a technique is described in this section for using an output

23

adder to obtain a desired sequence initiation.

In generating a desired initial n-tuple using an SSRG a "grand mod-2 adder" is used. This adder takes the outputs of selected stages and mod-2 adds them together to produce the total mod-2 sum. The grand adder has as many inputs as there are stages in the generator and the adder taps, α_i's, determine which stages are fed to the adder (see Fig. 4). If we let

$$\alpha_i = 1 \text{ if the i-th stage is fed to the adder}$$

$$= 0 \text{ otherwise} \tag{49}$$

and let x(j) be the output of the adder at time j, then

$$x(j) = \sum_{i=1}^{n} \alpha_i u_i(j) \quad (\text{mod-2}) \tag{50}$$

where $u_i(j)$ = contents of the i-th stage at time j. Define

$$X(j) = [x(j), x(j+1), \ldots, x(j+n-1)] \tag{51}$$

where x(j) = adder output at time j, and

$$\bar{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \tag{52}$$

then Eq. 50 can be written as

$$x(j) = \bar{\alpha} \, U(j) \quad (\text{mod-2}) \tag{53}$$

and Eq. 51 becomes

$$X(j) = \bar{\alpha} \cdot [U(j), U(j+1), \ldots, U(j+n-1)]_{n \times n} \quad (\text{mod-2}) \tag{54}$$

Assume that the output X(j) is desired when the contents of the generator consist of a single one in the first stage and zeros in all remaining stages. This special initial condition has been denoted $E_1(0)$ and is called the "first elementary load" (see Ref. 1). Therefore,

$$U(j) = E_1(0) \tag{55}$$

where

$$E_1(0) = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \qquad (56)$$

and

$$U(j+1) = A U(j) = A E_1(0) = E_1(1) \qquad (\text{mod-}2)$$

Equation 54 becomes

$$X(j) = \bar{\alpha}[E_1(0), E_1(1), \ldots, E_1(n-1)]_{n \times n} \qquad (\text{mod-}2) \qquad (57)$$

In Ref. 1, the n x n matrix on the right in Eq. 57 has been denoted as the E_A matrix associated with the SSRG, that is,

$$E_A = [E_1(0), E_1(1), \ldots, E_1(n-1)] \qquad (58)$$

Also in Ref. 1, a "feedback matrix," F_A, is defined for an SSRG. It has the form

$$F_A = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-3} & c_{n-2} & c_{n-1} \\ 0 & c_0 & c_1 & \cdots & c_{n-4} & c_{n-3} & c_{n-2} \\ 0 & 0 & c_0 & \cdots & c_{n-5} & c_{n-4} & c_{n-3} \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & c_0 & c_1 & c_2 \\ 0 & 0 & 0 & \cdots & 0 & c_0 & c_1 \\ 0 & 0 & 0 & \cdots & 0 & 0 & c_0 \end{bmatrix} \qquad (59)$$

where

c_j = feedback taps of the SSRG

$c_0 \equiv 1$.
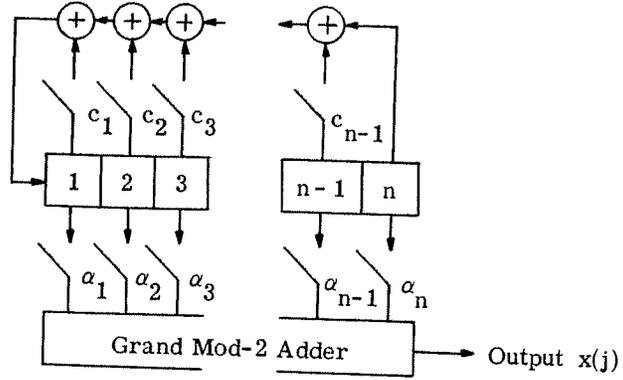
Fig. 4. Circuitry for generating a desired initial
n-tuple using an SSRG.

Furthermore, the E_A and F_A matrices are nonsingular matrices and are inverses,

$$E_A^{-1} = F_A \qquad (60)$$

From Eqs. 57, 58, and 60,

$$X(j) \, F_A = \bar{\alpha} \, E_A \, F_A = \bar{\alpha} \qquad (\text{mod-2}) \qquad (61)$$

In algebraic form, Eq. 61 becomes

$$\alpha_m = \sum_{k=1}^{m} c_{m-k} \, x(j+k-1) \qquad (\text{mod-2}) \qquad (62)$$

The solution (Eq. 62) guarantees that the output sequence starts with the desired n bits.

The sequences produced by each stage of a linear sequence generator obey the characteristic sequence law of the generator. Theorem 1 states that a sum sequence (consisting of the mod-2 sum of sequences each of which obey the same sequence law) obeys the same sequence law. Therefore, the output sequence X(j) from the grand adder in Fig. 4 obeys the sequence law of the generator and is determined by its first n bits. Consequently, by using the output adder circuit we can generate any desired sequence that obeys the characteristic sequence law of the generator. In a maximal SSRG, the adder output sequence X(j) will be the maximal sequence. In a nonmaximal generator, X(j) may be a completely different periodic sequence from that obtained as an output from any one of the stages of the generator.

26

4. THE MODULAR SHIFT-REGISTER GENERATOR

The modular shift-register generator (MSRG) was developed because of difficulty in the reliability of the SSRG at high frequencies. These high frequency problems of the SSRG arise from: (1) the unbalanced inputs to the mod-2 adders, and (2) from both time and propagation path delays. The treatment of the MSRG in this section will parallel the treatment given the SSRG in Section 3.

4.1 Definition

An SSRG is shown in Fig. 5(a). A "Modular Shift-Register Generator" (MSRG) is illustrated in Fig. 5(b). The term "Modular" stems from picturing the shift register of Fig. 5(b) as being composed of two types of modules (building blocks) sandwiched together. These modules are: (1) a single flip-flop capable of driving a single input, and (2) a flip-flop and mod-2 adder combination, capable of driving a single input. Figure 6(a) shows the building blocks and also the symbol which will be used to denote each. Using this representation, the MSRG of Fig. 5(b) with feedback switches c_0, c_1, and c_3 closed is depicted in Fig. 6(b). As shown, an amplifier for the final stage capable of driving n inputs is needed, since the modules (building blocks) are capable of driving only one input. For simplicity, the amplifier shown in Fig. 6(b) will be understood to be included and the representation for an MSRG will be as in Fig. 6(c).

The MSRG was developed to eliminate the difficulty encountered with SSRG's in experimental work because of unbalanced inputs; and at high frequencies because of the propagation time delay through feedback adders. The MSRG also permits a simplified method of interstage mod-2 addition (see Ref. 2). Since, as will be shown later, every linear generator has an equivalent MSRG, this new type of generator is important to consider.

As shown in Fig. 5(b), the switch c_0 is always closed (identically equal to one). This will be the only case considered in the following discussion on MSRG's because it is necessary for transient free operation (see Section 4.3). Also, the feedback switches have been numbered to correspond to the number of the shift stage directly <u>preceding</u> the switch.

(a) $c_j = 1$ if switch is closed

$= 0$ if switch is open

(b) $c_j = 1$ if switch is closed

$= 0$ if switch is open
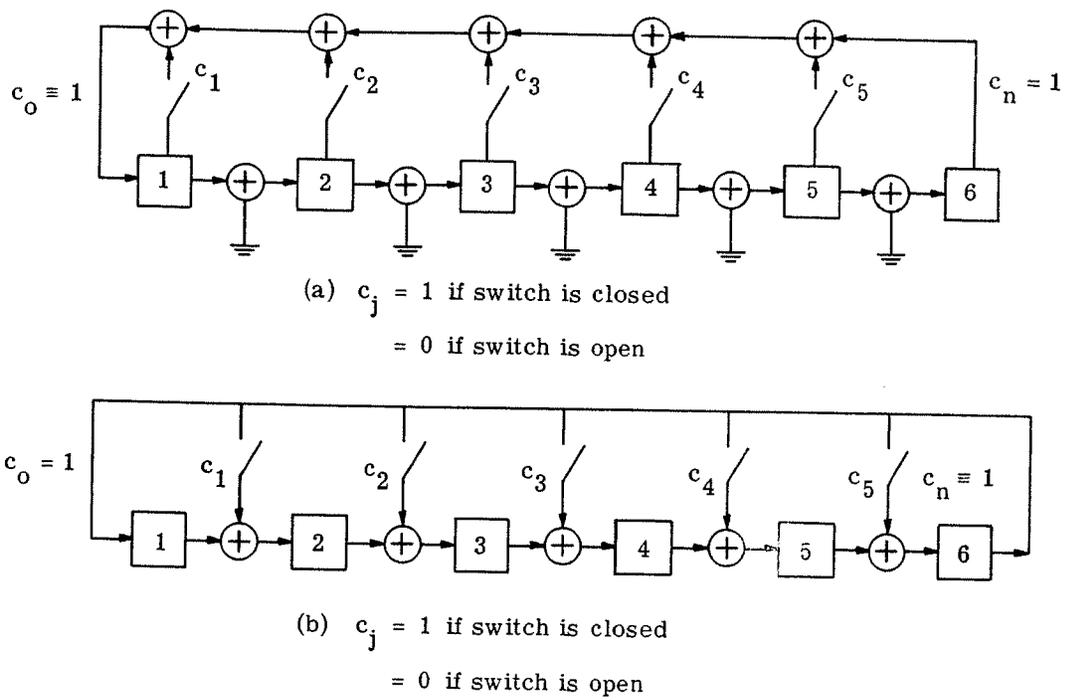
Fig. 5. General representations of SRG's: (a) general representation of an SSRG, (b) general representation of an MSRG.

Flip-Flop   Symbol

(b)

(a)

Flip-Flop and Adder   Symbol

(c)
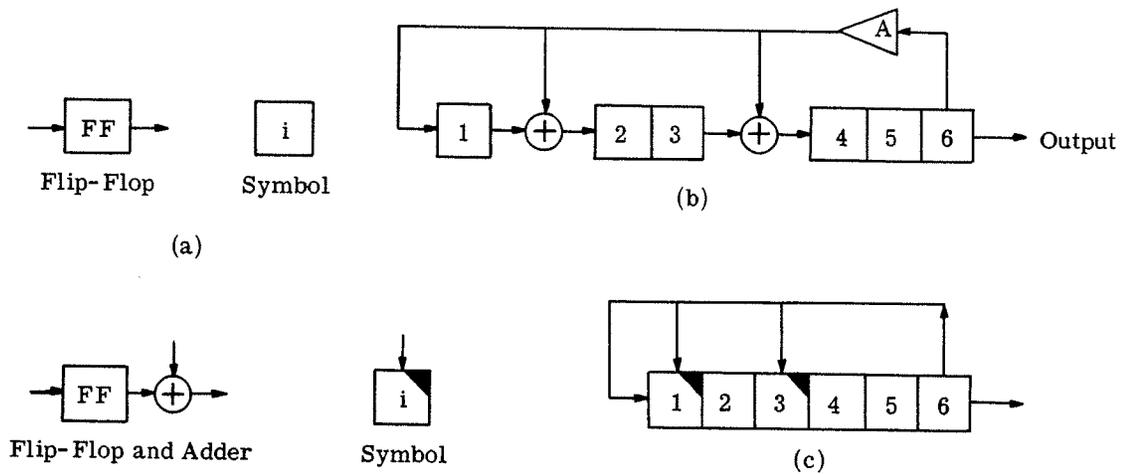
Fig. 6. Schematic representation of MSRG: (a) building blocks and corresponding symbol, (b) general representation of MSRG with feedback switches c_1 and c_3 closed, (c) schematic representation of (b).

28

That is, if $c_m = 1$ is a feedback tap, then this convention implies that the switch on the mod-2 adder following the m-th stage is closed.

In Fig. 5(b) the switches, denoted as c_i, represent the "feedback taps" of the MSRG.

$$
\left. \begin{array}{l}
c_i \;=\; 1 \quad \text{if both the i-th and the last} \\
\qquad\qquad \text{stage feed the (i+1)-th stage} \\[2mm]
\quad\; =\; 0 \quad \text{if only the i-th stage feeds the} \\
\qquad\qquad (i+1)\text{-th stage} \\[2mm]
c_0 \;=\; c_n \;\equiv\; 1
\end{array} \right\} \qquad (63)
$$

and

4.2 The "A" Matrix

From the feedback arrangement of the MSRG (Fig. 5b), it is obvious that the content of the i-th stage at time j, $u_i(j)$ is determined by the relationship

$$
\left. \begin{array}{l}
u_1(j) \;=\; c_0\, u_n(j-1) \;=\; u_n(j-1) \\[3mm]
u_i(j) \;=\; u_{i-1}(j-1) + c_{i-1}\, u_n(j-1) \quad (\text{mod-2}) \quad \text{for } i = 2,3,\ldots,n
\end{array} \right\} \qquad (64)
$$

and

By the definition of the A matrix in Eqs. 4 and 64, the A matrix for the MSRG has the form

$$
A \;=\; \begin{bmatrix}
0 & 0 & \cdots & 0 & 0 & c_0 \\
1 & 0 & \cdots & 0 & 0 & c_1 \\
0 & 1 & \cdots & 0 & 0 & c_2 \\
\vdots & \vdots & & \vdots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & 0 & c_{n-2} \\
0 & 0 & \cdots & 0 & 1 & c_{n-1}
\end{bmatrix} \qquad (65)
$$

29

That is,

$$A = [a_{i,j}]$$

where

$$
\left.
\begin{array}{l}
a_{i,n} = c_{i-1} \\
a_{i,i-1} \equiv 1 \\
a_{i,j} = 0, \text{ otherwise}
\end{array}
\right\} \tag{66}
$$

4.3 Characteristic Polynomial, Sequence Law, and Feedback Equation

From Eqs. 6 and 7, the characteristic polynomial is the determinate

$$f(\xi) = |A + I\xi| = \sum_{i=0}^{n} b_i \xi^i \quad (\text{mod-}2)$$

where $b_n \equiv 1$.

For the MSRG, the transpose of the A matrix, A^T, is a companion matrix having the form

$$
A^T = \begin{bmatrix}
0 & 1 & 0 & \cdots & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 \\
c_0 & c_1 & c_2 & \cdots & c_{n-2} & c_{n-1}
\end{bmatrix} \tag{67}
$$

Comparing Eq. 67 with Eq. 8, the characteristic polynomial of an MSRG is

$$f(\xi) = \sum_{i=0}^{n} c_i \xi^i \quad (\text{mod-}2) \tag{68}$$

From Eqs. 7 and 68, the characteristic polynomial for an MSRG is determined by the relationship

$$b_i = c_i \qquad i = 0, 1, 2, \ldots, n \tag{69}$$

where the b_i are the coefficients in the characteristic polynomial and the c_i are the feedback taps of the MSRG.

From Eqs. 14 and 69, the characteristic sequence law for an MSRG becomes

$$u_i(j) = \sum_{k=1}^{n} c_{n-k}\, u_i(j-k) \quad (\text{mod-}2) \qquad \text{for } i = 1,2,\ldots,n. \tag{70}$$

The feedback equation for an MSRG is defined similar to the feedback equation for an SSRG.

$$[n,a,b,\ldots,d,0]_{MS} : \quad \begin{array}{l} \text{\underline{Feedback equation} for an MSRG} \\ \text{with feedback taps } a,b,\ldots,d, \\ \text{and 0 closed. By convention } n \\ \text{is always closed.} \end{array} \tag{71}$$

Note that n, as well as 0, has been placed in the feedback equation to indicate that $c_0 = c_n \equiv 1$.

From Eqs. 23, 69, and 71, the characteristic polynomial and the feedback equation for an MSRG, are the same, that is

$$\text{characteristic polynomial} \Longleftrightarrow \text{feedback equation}$$
$$\tag{72}$$
$$(n,a,b,\ldots,c,0) \Longleftrightarrow [n,a,b,\ldots,c,0]_{MS}$$

For example, the six stage MSRG in Fig. 6(c) with feedback taps c_0, c_1, and c_3 closed has the feedback equation and the characteristic polynomial

$$[6,3,1,0]_{MS} \Longleftrightarrow (6,3,1,0)$$

The relationship between the feedback taps and the coefficients in the characteristic polynomial points out two important properties of MSRG's:

(1) Theorem 4 states that any periodic sequence from a generator with a characteristic polynomial having no constant term ($b_0 = 0$) can be generated by a generator with fewer than n stages. Therefore, since $c_0 = b_0$, any periodic sequence, from an MSRG for which $c_0 = 0$, can be generated by a generator with fewer than n stages.

31

(2) Theorem 3 states that if

$$\sum_{i=0}^{n} b_i = 0 \quad (\text{mod-2})$$

then $(\xi + 1)$ is a factor of $f(\xi)$ and the generator is nonmaximal.

For the MSRG $b_i = c_i$, thus

$$\sum_{i=0}^{n} b_i = \sum_{i=0}^{n} c_i \quad (\text{mod-2})$$

and if,

$$\sum_{i=0}^{n} c_i = 0 \quad (\text{mod-2})$$

then, $(\xi + 1)$ is a factor of $f(\xi)$. Hence, <u>for a maximal MSRG</u>

$$\sum_{i=0}^{n} c_i = 1 \quad (\text{mod-2}) \tag{73}$$

and every maximal MSRG must have an even number of feedback taps (not counting $c_n \equiv 1$).

4.4 Initial Loading

Like the SSRG, it is possible to find the initial loading of an MSRG so that a specified n-tuple of consecutive digits $u_n(j)$, $u_n(j+1)$, ..., $u_n(j+n-1)$ will be generated at the output of the n-th stage. From Eq. 64, but increasing all indices by $k + 1$,

$$u_{i+k+1}(j+k+1) = u_{i+k}(j+k) + c_{i+k}\, u_n(j+k) \quad (\text{mod-2})$$
$$\text{for } 1 - i \leq k \leq n - i - 1 \tag{74}$$

As long as we hold i to the range $1 \leq i \leq n - 1$, we may sum both sides over k, from $k = 0$ through $k = n - i - 1$

$$\sum_{k=0}^{n-i-1} u_{i+k+1}(j+k+1) = \sum_{k=0}^{n-i-1} u_{i+k}(j+k) + \sum_{k=0}^{n-i-1} c_{i+k}\, u_n(j+k) \quad (\text{mod-2}) \tag{75}$$

The first two sums have many terms in common. Subtracting these we obtain

$$u_n(j+n-i) = u_i(j) + \sum_{k=0}^{n-i-1} c_{i+k}\, u_n(j+k) \quad (\text{mod-2}) \tag{76}$$

32

Because $c_n = 1$ for a nontransient generator, we see that the left-hand side can be absorbed by the sum for the index $k = n - i$

$$u_i(j) = \sum_{k=0}^{n-i} c_{i+k} u_n(j+k) \qquad 1 \le i \le n - 1 \qquad (\text{mod-}2) \qquad (77)$$

Now Eq. 77 trivially holds for $i = n$, since the sum will then only be the $k = 0$ term $c_n u_n(j)$. We, therefore, have the desired result

$$u_i(j) = \sum_{k=0}^{n-i} c_{i+k} u_n(j+k) \qquad 1 \le i \le n \qquad (\text{mod-}2) \qquad (78)$$

which relates the initial load $u_1(j)$, $u_2(j)$, ..., $u_n(j)$ to the initial output n-tuple $u_n(j)$, $u_n(j+1)$, ..., $u_n(j+n-1)$.

If F_M is defined by the equation

$$F_M = \begin{bmatrix} c_1 & c_2 & c_3 & \cdots & c_{n-2} & c_{n-1} & c_n \\ c_2 & c_3 & c_4 & \cdots & c_{n-1} & c_n & 0 \\ c_3 & c_4 & c_5 & \cdots & c_n & 0 & 0 \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ c_{n-2} & c_{n-1} & c_n & \cdots & 0 & 0 & 0 \\ c_{n-1} & c_n & 0 & \cdots & 0 & 0 & 0 \\ c_n & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix} \qquad (79)$$

then Eq. 78 can be written in matrix form as

$$U(j) = F_M V_n(j) \qquad (\text{mod-}2) \qquad (80)$$

where $U(j)$ and $V_n(j)$ are as defined in Eqs. 1 and 15, respectively, and $V_n(j)$ is the desired initial output n-tuple.

From Eq. 70 or 72, the feedback equation for an MSRG can be found for any sequence law or characteristic polynomial. From Eq. 78 or 80, the necessary initial loading for the MSRG can be determined to generate a desired n-tuple of consecutive bits as the starting output of the last stage. Hence, by Section 2.6

33

Theorem 6

Any sequence that can be generated by an n-stage linear sequence generator can be generated by an n-stage MSRG.

Corollary

Every SSRG has an equivalent MSRG, and vice versa. From Eqs. 41 and 72, the relationship between the equivalent SSRG and MSRG becomes

$$[n, a, b, \ldots, d, 0]_{MS} \iff [n, n-d, \ldots, n-b, n-a, 0]_{SS}$$

or

$$[n, a, b, \ldots, d, 0]_{SS} \iff [n, n-d, \ldots, n-b, n-a, 0]_{MS} \tag{81}$$

Notice that the equivalence relationship in Eq. 81 is a simple reverse of the feedback equation.

4.5 Interstage Relationships

The relationship between the output sequences from different stages of an MSRG differs from that of an SSRG in that there exists a jump or change in the sequences whenever two stages are separated by an interstage mod-2 adder. This phenomenon is related to the shift-and-add property of sequences, consequently, it is convenient to consider maximal and nonmaximal MSRG's separately.

4.5.1 Maximal MSRG.

In a maximal MSRG every stage produces the same maximal sequence but they are shifted in time from one another. If two successive stages, say the i-th and the (i+1)-th, are not separated by an interstage adder, and if $X_i(j)$ represents the sequence produced by the i-th stage, then

$$X_i(j) = X_{i+1}(j+1) \tag{82}$$

If the two stages are separated by an interstage adder, then

$$X_i(j) = X_{i+1}(j+1) + X_n(j) \quad (\text{mod-}2)$$

$$X_i(j) = X_{i+1}(j + J_{i, i+1}) \tag{83}$$

where $J_{i, i+1}$ is a time shift related to the shift-and-add property of maximal sequences.

34

The following discussion develops one method for determining the shift $J_{i,n}$ between the sequences from the i-th stage and the n-th stage of a maximal MSRG.

Let $V_i(j)$ be an n-tuple of digits from the sequence $X_i(j)$ with time reference j, that is

$$
V_i(j) \;=\; \begin{bmatrix} u_i(j) \\ u_i(j+1) \\ \cdot \\ \cdot \\ \cdot \\ u_i(j+n-1) \end{bmatrix}
$$

From Eq. 16, repeated here,

$$
C_f^k \; V_i(j) \;=\; V_i(j+k) \qquad (\text{mod-2}) \tag{16}
$$

where C_f is the companion matrix associated with the characteristic polynomial of the MSRG. From Eq. 64, we can write

$$
u_i(j) \;=\; u_{i+1}(j+1) + c_i\, u_n(j) \qquad (\text{mod-2}) \qquad \text{for } i = 1,2,\ldots,n-1
$$

from which follows

$$
V_i(j) \;=\; V_{i+1}(j+1) + c_i\, V_n(j) \qquad (\text{mod-2}) \qquad 1 \le i \le n-1 \tag{84}
$$

Let $J_{i,n}$ be the time shift between the sequences produced by the i-th stage and the n-th stage so that

$$
V_i(j) \;=\; V_n(j+J_{i,n}) \tag{85}
$$

then using Eqs. 85, 84, and 16

$$
\begin{aligned}
V_{n-1}(j) &= V_n(j+J_{n-1,n}) \\
&= C_f^{J_{n-1,n}} \; V_n(j) \qquad (\text{mod-2}) \\
&= V_n(j+1) + c_{n-1}\, V_n(j) \qquad (\text{mod-2}) \\
&= (C_f + c_{n-1} I)\, V_n(j) \qquad (\text{mod-2})
\end{aligned}
$$

35

$J_{n-1,n}$ is the solution to the equation

$$C_f^{J_{n-1,n}} = C_f + c_{n-1} I \quad (\text{mod-2}) \tag{86}$$

Similarly,

$$V_{n-2}(j) = V_n(j + J_{n-2,n})$$

$$= C_f^{J_{n-2,n}} V_n(j) \quad (\text{mod-2})$$

$$= V_{n-1}(j+1) + c_{n-2} V_n(j) \quad (\text{mod-2})$$

$$= [C_f(C_f + c_{n-1} I) + c_{n-2} I] V_n(j) \quad (\text{mod-2})$$

$$= (C_f^2 + c_{n-1} C_f + c_{n-2} I) V_n(j) \quad (\text{mod-2})$$

and $J_{n-2,n}$ is the solution to the equation

$$C_f^{J_{n-2,n}} = C_f^2 + c_{n-1} C_f + c_{n-2} I \quad (\text{mod-2}) \tag{87}$$

Assume that for some arbitrary value of i, $J_{n-i,n}$ is the solution to the equation

$$C_f^{J_{n-i,n}} = c_n C_f^i + c_{n-1} C_f^{i-1} + \ldots + c_{n-i+1} C_f + c_{n-i} I \quad (\text{mod-2}) \tag{88}$$

then

$$V_{n-i-1}(j) = V_n(j + J_{n-i-1,n})$$

$$= C_f^{J_{n-i-1,n}} V_n(j) \quad (\text{mod-2})$$

$$= V_{n-i}(j+1) + c_{n-i-1} V_n(j) \quad (\text{mod-2})$$

$$= V_n(j + J_{n-i,n} + 1) + c_{n-i-1} V_n(j) \quad (\text{mod-2})$$

$$= (C_f \cdot C_f^{J_{n-i,n}} + c_{n-i-1} I) V_n(j) \quad (\text{mod-2})$$

$$= (c_n C_f^{i+1} + c_{n-1} C_f^i + \ldots + c_{n-i} C_f + c_{n-i-1} I) V_n(j) \quad (\text{mod-2})$$

and $J_{n-i-1,n}$ is the solution to the equation

$$C_f^{J_{n-i-1,n}} = c_n C_f^{i+1} + c_{n-1} C_f^i + \ldots + c_{n-i} C_f + c_{n-i-1} I \quad (\text{mod-2}) \tag{89}$$

36

From Eq. 89, if Eq. 88 is true for some particular value of i, then it is true for the next larger value of i. From Eqs. 86 and 87, Eq. 88 is true for i = 1 and i = 2 since $c_n \equiv 1$. Therefore, by induction, Eq. 88 is true for $1 \leq i \leq n - 1$. The solution to Eq. 88 can be determined from the B_A matrix for the characteristic polynomial. Since the characteristic polynomial for C_f is the same as that for the A matrix of the MSRG, $J_{n-i,\,n}$ can be considered as the solution to the equation

$$A^{J_{n-i,\,n}} = c_n A^i + c_{n-1} A^{i-1} + \ldots + c_{n-i+1} A + c_{n-i} I \qquad (\text{mod-}2) \qquad (90)$$

As an example consider a $[4,3,0]_{MS}$ maximal MSRG. Figure 7 shows this generator and its periodic sequences along with its associated B_A matrix.

	1	2	3	4		Powers of A	3	2	1	0
	1	0	0	0		1	0	0	1	0
	0	1	0	0		2	0	1	0	0
	0	0	1	0		3	1	0	0	0
	0	0	0	1		4	1	0	0	1
	1	0	0	1		5	1	0	1	1
	1	1	0	1		6	1	1	1	1
	1	1	1	1		7	0	1	1	1
	1	1	1	0		8	1	1	1	0
	0	1	1	1		9	0	1	0	1
	1	0	1	0		10	1	0	1	0
	0	1	0	1		11	1	1	0	1
	1	0	1	1		12	0	0	1	1
	1	1	0	0		13	0	1	1	0
	0	1	1	0		14	1	1	0	0
	0	0	1	1		15	0	0	0	1
	1	0	0	0						
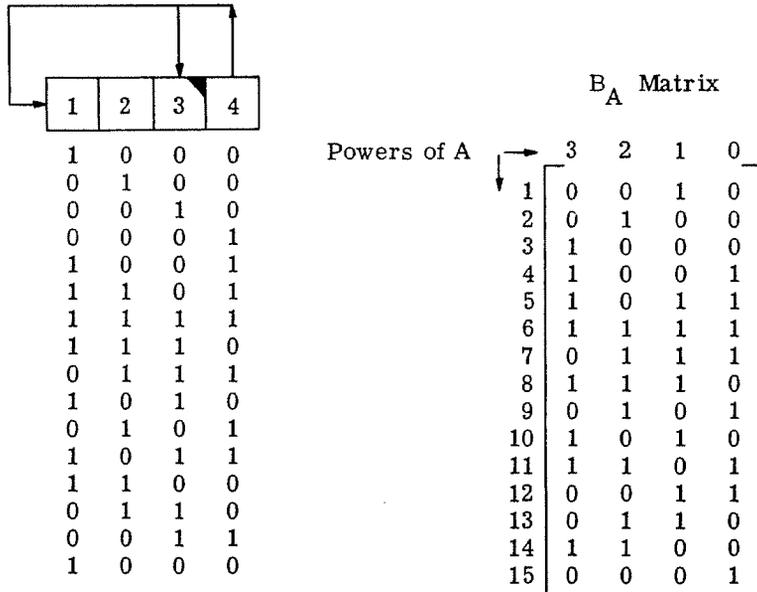
B_A Matrix

Fig. 7. The $[4,3,0]_{MS}$ MSRG and the associated B_A matrix.

Applying Eq. 90 and the B_A matrix

$$A^{J_{3,4}} = c_4 A + c_3 I = A + I = A^{12} \qquad (\text{mod-}2)$$

$$A^{J_{2,4}} = c_4 A^2 + c_3 A + c_2 I = A^2 + A = A^{13} \qquad (\text{mod-}2)$$

$$A^{J_{1,4}} = c_4 A^3 + c_3 A^2 + c_2 A + c_1 I = A^3 + A^2 = A^{14} \qquad (\text{mod-}2)$$

37

so

$$J_{1,4} = 14$$

$$J_{2,4} = 13$$

$$J_{3,4} = 12$$

and

$$X_1(j) = X_4(j + 14) = X_4(j - 1)$$

$$X_2(j) = X_4(j + 13) = X_4(j - 2)$$

$$X_3(j) = X_4(j + 12) = X_4(j - 3)$$

These shifts are verified from the sequences shown in Fig. 7.

The shift between successive stages $J_{i,i+1}$ can be obtained from the values of $J_{i,n}$ in the following manner: if,

$$J_{i+1,n} < J_{i,n} \qquad 1 \le i \le n - 2$$

then,

$$J_{i,i+1} = J_{i,n} - J_{i+1,n} \tag{91}$$

However, if

$$J_{i+1,n} > J_{i,n}$$

then,

$$J_{i,i+1} = L - J_{i+1,n} + J_{i,n} \tag{92}$$

where

$$L = 2^n - 1 = \text{the length of the maximal sequence } X_i$$

For the above example,

$$J_{1,2} = 1$$

$$J_{2,3} = 1$$

$$J_{3,4} = 12$$

or

$$X_1(j) = X_2(j + 1)$$

$$X_2(j) = X_3(j + 1)$$

$$X_3(j) = X_4(j + 12)$$

That is, the shift between sequences not separated by an adder is 1, as predicted by Eq. 82. The shift between sequences separated by an interstage adder is some value $J_{i,i+1}$ determined by the shift-and-add property of maximal sequences, as predicted by Eq. 83.

Tables of the shift between sequences from adjacent stages for all maximal MSRG's of length $2 \leq n \leq 12$ are given in Section 8.4.

4.5.2 Nonmaximal MSRG. Like the maximal MSRG, if two stages of a non-maximal MSRG are not separated by an interstage adder then they will produce the same sequence. However, the time index will be shifted by one, that is, $X_i(j) = X_{i+1}(j+1)$. If the two stages are separated by an adder, then they may produce the same sequence shifted in time. Or they may produce completely different sequences, depending upon the partial shift-and-add property of the nonmaximal sequence.

4.6 A B_A Matrix Generator[5]

The relationship between the stage contents of an MSRG and the B_A matrix associated with the characteristic polynomial of that MSRG is useful and interesting.

Let the characteristic polynomial of the MSRG be

$$f(\xi) = b'_n \xi^n + b'_{n-1} \xi^{n-1} + \ldots + b'_1 \xi + b'_0 \quad (\text{mod-2}) \tag{93}$$

where $b'_n \equiv 1$. (The coefficients have primes to help avoid confusion with the elements of

---

[5]Ref. 2, p. 25.

39

the B_A matrix.) From the Cayley-Hamilton Theorem, (Ref. 3) a matrix satisfies its own characteristic equation so that

$$A^n = \sum_{j=1}^{n} b'_{n-j} A^{n-j} \quad (\text{mod-}2) \tag{94}$$

From the definition of the B_A matrix (Section 2.5), Eqs. 29 and 30

$$B_A = [b_{i,j}]_{\ell \times n} \tag{29}$$

where the $b_{i,j}$'s are the coefficients in the equation

$$A^i = \sum_{j=1}^{n} b_{i,j} A^{n-j} \quad (\text{mod-}2) \tag{30}$$

Consider A^{k+1}, applying Eq. 30

$$A^{k+1} = \sum_{j=1}^{n} b_{k+1,j} A^{n-j} \quad (\text{mod-}2)$$

$$= \sum_{j=1}^{n-1} b_{k+1,j} A^{n-j} + b_{k+1,n} I \quad (\text{mod-}2) \tag{95}$$

also consider A^{k+1} in the following manner, from Eqs. 30 and 94:

$$A^{k+1} = A \cdot A^k \quad (\text{mod-}2)$$

$$= A \left(\sum_{j=1}^{n} b_{k,j} A^{n-j} \right) \quad (\text{mod-}2)$$

$$= \sum_{j=2}^{n} b_{k,j} A^{n-j+1} + b_{k,1} A^n \quad (\text{mod-}2)$$

$$= \sum_{j=1}^{n-1} b_{k,j+1} A^{n-j} + b_{k,1} \sum_{j=1}^{n} b'_{n-j} A^{n-j} \quad (\text{mod-}2)$$

$$= \sum_{j=1}^{n-1} (b_{k,j+1} + b_{k,1} b'_{n-j}) A^{n-j} + b_{k,1} b'_0 I \quad (\text{mod-}2) \tag{96}$$

Equating Eqs. 95 and 96, the following relationship is obtained

$$k \geq 1 \begin{cases} b_{k+1,j} = b_{k,j+1} + b_{k,1} b'_{n-j} \quad (\text{mod-}2) \quad 1 \leq j \leq n-1 \\ \\ \\ b_{k+1,n} = b_{k,1} b'_0 \end{cases} \tag{97}$$

40

Consider now an n-stage MSRG with the characteristic polynomial given in Eq. 93. For an MSRG, from Eq. 69

$$c_i = b_i', \quad i = 0, 1, \ldots, n$$

where the c_i's are the feedback taps and the b_i''s are the coefficients in the characteristic polynomial. Equation 64 can be rewritten

$$\left.\begin{array}{l} u_1(k+1) = b_0' u_n(k) \\[2ex] u_{n-j+1}(k+1) = u_{n-j}(k) + b_{n-j}' u_n(k) \quad (\text{mod-2}) \quad 1 \leq j \leq n-1 \end{array}\right\} \quad (98)$$

From the definition of the B_A matrix

$$A^1 = \sum_{j=1}^{n} b_{1,j} A^{n-j} = A \quad (\text{mod-2})$$

which requires

$$\left.\begin{array}{l} b_{1,n-1} = 1 \\[2ex] b_{1,j} = 0 \quad \text{for } j \neq n-1 \end{array}\right\} \quad (99)$$

Assume that the MSRG is initially loaded at time $k = 0$ with a one in the first stage and zeros in all remaining stages; that is,

$$u_{n-j+1}(0) = \delta_{0,n-j} \quad \left.\begin{array}{l} = 1 \text{ when } j = n \\[2ex] = 0 \text{ when } j \neq n \end{array}\right\} \quad (100)$$

From Eqs. 98, 99, and 100, for $n > 1$

41

$$u_1(1) = b_0' \, u_n(0) = b_0' \, \delta_{0,n-1} = 0 = b_{1,n}$$

$$u_{n-j+1}(1) = u_{n-(j+1)+1}(0) + b_{n-j}' \, u_n(0) \qquad (\text{mod-2})$$

$$= \delta_{0,n-j-1} + b_{n-j}' \cdot \delta_{0,n-1} \qquad (\text{mod-2})$$

$$= \delta_{0,n-j-1} + 0$$

$$= \delta_{1,n-j} \qquad 1 \le j \le n-1$$

$$= b_{1,j}$$

<div style="text-align:right">(101)</div>

Thus,

$$u_{n-j+1}(1) = b_{1,j} \quad \text{for} \quad j = 1, 2, \ldots, n$$

or

$$u_{n-j+1}(k) = b_{k,j} \quad \text{for } k = 1; \quad 1 \le j \le n \tag{102}$$

Equation 102 can be shown by induction to be true for all $k \ge 1$ in the following manner: Assume that Eq. 102 is true for $k = m$, then from Eqs. 97 and 98,

$$u_{n-j+1}(m+1) = u_{n-(j+1)+1}(m) + b_{n-j}' \, u_n(m) \qquad (\text{mod-2})$$

$$= b_{m,j+1} + b_{n-j}' \, b_{m,1} \qquad (\text{mod-2})$$

$$= b_{m+1,j} \qquad \text{for} \quad 1 \le j \le n-1 \tag{103}$$

and

$$u_1(m+1) = b_0' \, u_n(m)$$

$$= b_0' \, b_{m,1}$$

$$= b_{m+1,n} \tag{104}$$

Combining Eqs. 103 and 104

$$u_{n-j+1}(m+1) = b_{m+1,j} \qquad \text{for} \quad 1 \leq j \leq n \qquad (105)$$

We have shown that if Eq. 102 is true for some value of k, then by Eq. 105 it is also true for the next larger value of k, and, therefore, by induction

$$u_{n-j+1}(k) = b_{k,j}; \qquad \text{for} \quad 1 \leq j \leq n \quad \text{and} \quad k \geq 1 \qquad (106)$$

From Eq. 106, it is seen that if the MSRG is initially loaded at time k = 0 with

$$u_1(1) = 1$$

$$u_i(1) = 0 \quad \text{for} \quad i \neq 1$$

then at time $k \geq 1$, the contents of the MSRG are the elements of the k-th row of the B_A matrix read as indicated in Eq. 106.

A B_A matrix computer can be constructed as shown in Fig. 8 by applying this result: The computer operates in this way: The pulser shifts the MSRG, and at the same time, shifts the "line advance" for the printer. The printer records the digital contents of each stage for each shift. The net effect is to print the B_A matrix one row at a time. For work in which the B_A matrix is required (n large), such a computer is a great labor saving device, since writing out the B_A matrix by hand is lengthy for large n.
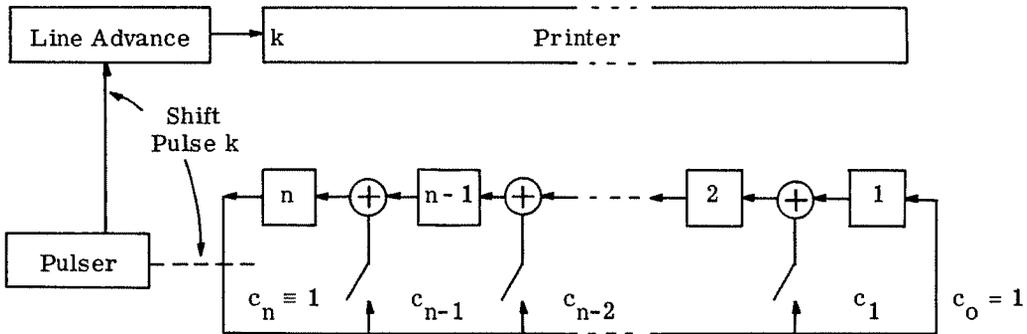
Fig. 8. A B_A matrix computer.

4.7 Output Adder Circuit

An output adder circuit can be used with an MSRG in the same manner that it is used with an SSRG to obtain a particular sequence or, equivalently, a particular initial n-tuple as an output from the adder. The MSRG and the output grand mod-2 adder are shown in Fig. 9. It is assumed the n-tuple output is desired when the MSRG contents are the elementary load $E_1(0)$ (see Eq. 56).

Suppose that the MSRG is loaded at time j with a one in the first stage and zeros in all the remaining stages; that is

$$u_i(j) = \delta_{0, i-1} = 1 \quad \text{when } i - 1 = 0$$
$$= 0 \quad \text{otherwise}$$

For this initial loading, using Eq. 106,

$$u_i(j+k) = b_{k, n-i+1} \quad \text{for} \quad k \geq 1$$

where $b_{k, j}$ is the element of the k-th row and the j-th column of the B_A matrix. For $k \leq n-1$,

$$A^k = \sum_{j=1}^{n} b_{k, j} A^{n-j} = A^k \quad \text{(mod-2)}$$

and, thus,

$$b_{k, j} = \delta_{k, n-j} = 1 \quad \text{when } j = n-k, \quad k \leq n-1$$
$$= 0 \quad \text{when } j \neq n-k$$

and for $k \leq n-1$

$$\left. \begin{aligned} u_i(j+k) &= b_{k, n-i+1} \\ &= \delta_{k, i-1} = 1 \quad \text{when } i - 1 = k \\ &= 0 \quad \text{when } i - 1 \neq k \end{aligned} \right\} \quad (107)$$

The output $x(j+k)$ of the adder in Fig. 9 is given by

$$x(j+k) = \sum_{i=1}^{n} \alpha_i u_i(j+k) \quad \text{(mod-2)}$$

44
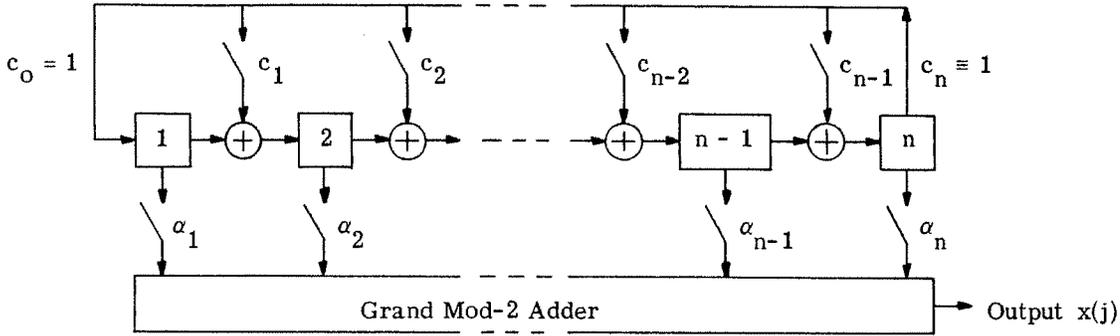
Fig. 9. An MSRG with an output adder circuit.

From Eq. 107, for $k \leq n-1$

$$x(j+k) = \sum_{i=1}^{n} \alpha_i \, \delta_{k, i-1} \quad (\text{mod-}2)$$

$$= \alpha_{k+1}$$

If $x(j)$, $x(j+1), \ldots, x(j+n-1)$ are the first n digits of the sequence desired as an output of the adder when $U(j) = E_1(0)$, the adder taps which should be closed can be found from the equation

$$\alpha_k = x(j+k-1) \quad \text{for} \quad k = 1, 2, \ldots, n \tag{108}$$

If this is written in matrix form using the notation

$$X(j) = [x(j), \; x(j+1), \ldots, x(j+n-1)]$$

and

$$\overline{\alpha} = [\alpha_1, \alpha_2, \ldots, \alpha_n]$$

Eq. 108 becomes

$$\overline{\alpha} = X(j) \tag{109}$$

45

This section completes the discussion of shift-register generators.[6] As we pointed out in Section 1, "complement stages" can be employed rather than shift stages to form complement-register generators. Two forms of complement-register generators will now be considered: the simple complement-register generator which has a form similar to the SSRG; and the modular complement-register generator, which is analogous to the MSRG.

---

[6]Except for Section 8. In Section 8 some of the advantages of the various types of generators are discussed and a comparison is made of the properties of each.

5. THE SIMPLE COMPLEMENT REGISTER GENERATOR

A linear sequence generator can be constructed using complement stages (binary counter stages) rather than the shift stages used in the SSRG and MSRG. The difference in operation between the shift stage and complement stage is: the shift stage directly stores its input, whereas the content of a complement stage remains unchanged when its input is a "0" and is changed or "complemented" when its input is "1". The operation of a complement stage is equivalent to adding (mod-2) the input to the complement stage to its present content. This sum then forms the new contents of the complement stage. Consequently, the complement stage can be considered as a shift stage which has a feedback loop from its output to its input as shown in Fig. 10. We will use this analogy in this report in discussing the development of the theory of complement-register generators.

Input ⟶ | i | ⟶ Output

Shift Stage

Input ⟶ | i_c | ⟶ Output ⟺ Input ⟶ (+) ⟶ | i | ⟶ Output
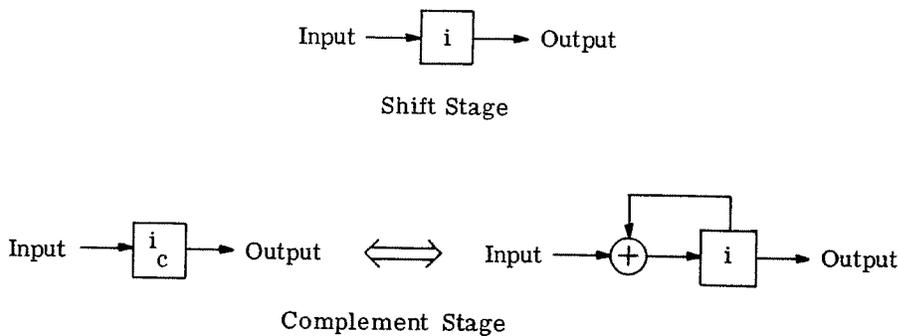
Complement Stage

Fig. 10. A shift stage and a complement stage.

A linear sequence generator which is made up entirely of complement stages instead of shift stages will be called a complement-register generator (CRG). Figure 11(a) shows an arbitrary multiple return CRG. Figure 11(b) shows an equivalent generator using shift stages.

Why consider other types of generators when, as shown in Sections 3 and 4, any linear sequence can be generated by either an SSRG or an MSRG? There are two reasons

47

for developing the theory of complement register generators: (1) the complement stage physically requires fewer components to construct than the shift stage; and, (2) the interconnection between the stages is simpler. Today, with emphasis placed on size, weight, and cost of generators, the advantages of the CRG are obvious. Also, the CRG has some additional properties which add to its usefulness. (See Section 8.)
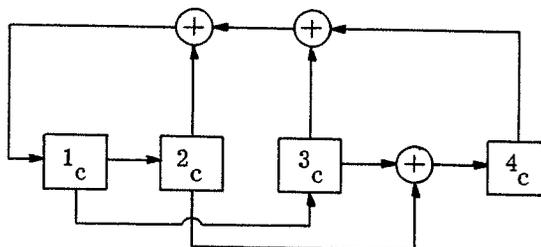
(a) Complement-Register Generator
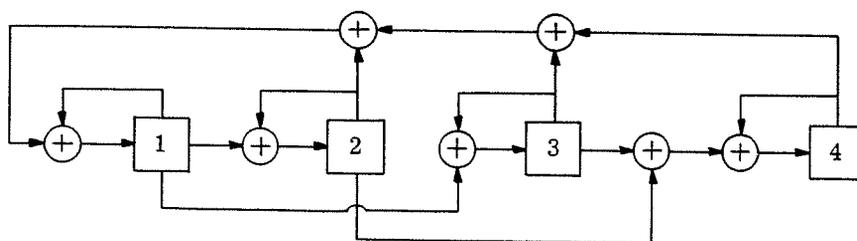
(b) Shift-Register Generator

Fig. 11. Two representations of the same
multiple return generator.

In this section we will develop the theory for one particular type of complement register generator, namely, the simple-complement-register-generator (SCRG). The treatment we use follows closely that of Sections 3 and 4. In Section 6, we will treat the "modular-complement-register-generator" (MCRG).

5.1 Definition

A simple-complement-register generator (SCRG) is a linear sequence generator which is constructed in the same manner as the SSRG except that the shift stages are replaced by complement stages. The general form of the SCRG is shown in Fig. 12(a). Note that in the SCRG (as with the SSRG) all feedback is to the first stage. A particular six-stage SCRG is shown in Fig. 12(b).

48
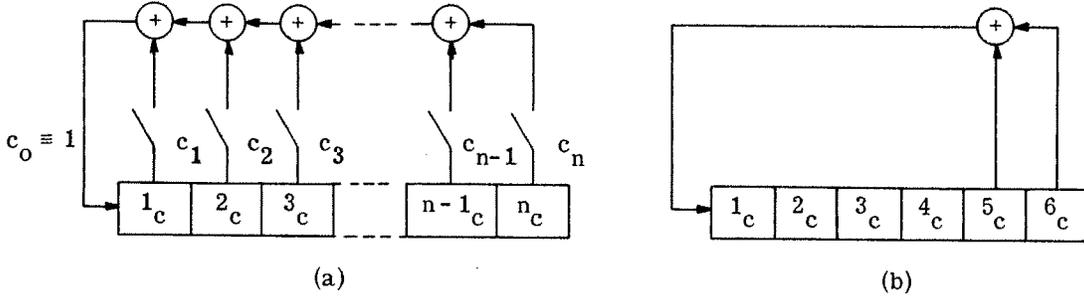
Fig. 12. a) The general form of an SCRG, (b) a $[6, 5, 0]_{SC}$ SCRG.

The operation of the SCRG is similar to that of the SSRG. Every stage except the first is fed by the previous stage, and the first stage is fed by the stages in the feedback loop. The c_i's in Fig. 12 represent the feedback taps where

$$\left.\begin{array}{l} c_i = 1 \text{ if the i-th stage feeds the 1st stage} \\[2ex] = 0 \text{ if the i-th stage does not feed the 1st stage} \end{array}\right\} \quad (110)$$

5.2 The A Matrix

Let $u_i(j)$ represent the contents of the i-th stage of an SCRG at time j. Then, by inspection of the SCRG in Fig. 12, using the shift stage analogy of Fig. 10, $u_i(j)$ can be expressed as

$$\left.\begin{array}{l} u_1(j) = u_1(j-1) + \displaystyle\sum_{i=1}^{n} c_i u_i(j-1) \quad \text{(mod-2)} \\[3ex] u_i(j) = u_i(j-1) + u_{i-1}(j-1) \quad \text{(mod-2)} \quad 2 \leq i \leq n \end{array}\right\} \quad (111)$$

Using the definition of the A matrix (Eq. 4), the A matrix for an SCRG has the form

$$A = \begin{bmatrix} 1+c_1 & c_2 & c_3 & \cdots & c_{n-2} & c_{n-1} & c_n \\ 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{bmatrix} \quad (112)$$

49

$$A = [a_{i,j}]$$

where

$$a_{1,1} = 1 + c_1 \qquad (\text{mod-}2)$$

$$a_{1,j} = c_j \qquad 2 \leq j \leq n$$

$$a_{j,j} = 1 \qquad 2 \leq j \leq n$$

$$a_{j,j-1} = 1 \qquad 2 \leq j \leq n$$

otherwise,

$$a_{i,j} = 0$$

$$(113)$$

5.3 Prefatory Note

Several special matrices are useful in developing the theory for CRG's. The "mod-2 binomial coefficients" also arise in this theory. These matrices and coefficients will be defined in this section to facilitate the subsequent presentation of the theory of CRG's.

5.3.1 The Mod-2 Binomial Coefficients, $(d_i)_k$.

The coefficients in the mod-2 binomial expansion play an important role in the development of the theory of complement-register generators. A brief description of these coefficients follows:

The expansion of the quantity $(x+1)^k$ can be expressed in terms of the binomial expansion:

$$(x + 1)^k = \binom{k}{k} x^k + \binom{k}{k-1} x^{k-1} + \ldots + \binom{k}{1} x + \binom{k}{0}$$

where

$$\binom{k}{r} \equiv \frac{k!}{r!(k-r)!} = \text{the binomial coefficient} \qquad (114)$$

50

The binomial coefficients $\binom{k}{r}$ have the following properties[7]:

$$\left.\begin{array}{c} \binom{k}{k} = \binom{k}{0} = 1 \\[2mm] \binom{k}{i} = \binom{k}{k-i} \\[2mm] \binom{k+1}{i} = \binom{k}{i} + \binom{k}{i-1} \end{array}\right\} \tag{115}$$

Define $(d_i)_k$ to be the "mod-2 binomial coefficient"; that is,

$$(d_i)_k \equiv \binom{k}{i} \quad (\text{mod-2}) \tag{116}$$

In other words,

$$(d_i)_k = 1 \text{ when } \binom{k}{i} \text{ is odd}$$
$$= 0 \text{ when } \binom{k}{i} \text{ is even} \tag{117}$$

In terms of $(d_i)_k$, the mod-2 binomial expansion of the quantity $(x+1)^k$ has the form

$$(x + 1)^k = \sum_{i=0}^{k} (d_i)_k \, x^i \quad (\text{mod-2}) \tag{118}$$

where $(d_i)_k$ has the properties[8]:

$$\left.\begin{array}{c} (d_k)_k = (d_0)_k = 1 \\[2mm] (d_i)_k = (d_{k-i})_k \\[2mm] (d_i)_{k+1} = (d_i)_k + (d_{i-1})_k \quad (\text{mod-2}) \quad 1 \le i \le k \end{array}\right\} \tag{119}$$

<u>5.3.2 I^*, R_i Matrices.</u> There are four nonsingular matrices composed of the mod-2 binomial coefficients which are important in the development of the theory of complement-register generators. These matrices are denoted R_1, R_2, R_3, and R_4. Another matrix, denoted I^*, arises in relating the R_i matrices to each other. These matrices are introduced below and the relationships between them are given. A complete discussion of this is reserved for Appendix B.

---

[7]See Ref. 4, pp. 33 and 49.

[8]These properties follow directly from the definition of $(d_i)_k$ and from the properties of $\binom{k}{r}$ in Eq. 115.

Define I* as

$$I^* = I \text{ rotated } 90^\circ = [i^*_{j,k}]_{n \times n}$$

where

$$i^*_{j,k} = \delta_{j,n+1-k} = 1 \text{ when } j = n + 1 - k$$

$$= 0 \text{ when } j \neq n + 1 - k$$

(120)

That is, I* has the form

$$I^* = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{bmatrix}$$

(121)

In Appendix B it is shown that[9]

$$I^* = (I^*)^{-1} = (I^*)^T$$

(122)

Define R_1 as

$$R_1 = [r^1_{i,j}]_{n \times n}$$

where

$$r^1_{i,j} = \begin{cases} (d_{j-1})_{i-1} & \text{for } j \leq i \\ \\ 0 & \text{for } j > i \end{cases}$$

(123)

That is, R_1 has the form

$$R_1 = \begin{bmatrix} (d_0)_0 & 0 & \cdots & 0 & 0 \\ (d_0)_1 & (d_1)_1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ (d_0)_{n-2} & (d_1)_{n-2} & \cdots & (d_{n-2})_{n-2} & 0 \\ (d_0)_{n-1} & (d_1)_{n-1} & \cdots & (d_{n-2})_{n-1} & (d_{n-1})_{n-1} \end{bmatrix}$$

(124)

[9] For any matrix M, the "transpose of the matrix" is denoted M^T.

In Appendix B it is shown that R_1 is "involutory," that is,

$$R_1^{-1} = R_1 \qquad (125)$$

Define R_2 as

$$R_2 = [r^2_{i,j}]_{n \times n}$$

where

$$r^2_{i,j} = \begin{cases} (d_{i-1})_{j-1} & \text{for } i \leq j \\ \\ 0 & \text{for } i > j \end{cases} \qquad (126)$$

That is, R_2 has the form

$$R_2 = \begin{bmatrix} (d_0)_0 & (d_0)_1 & \cdots & (d_0)_{n-2} & (d_0)_{n-1} \\ 0 & (d_1)_1 & \cdots & (d_1)_{n-2} & (d_1)_{n-1} \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ 0 & 0 & \cdots & (d_{n-2})_{n-2} & (d_{n-2})_{n-1} \\ 0 & 0 & \cdots & 0 & (d_{n-1})_{n-1} \end{bmatrix} \qquad (127)$$

In Appendix B it is shown that

$$R_2^{-1} = R_2 \qquad (128)$$

In addition, note that

$$R_2 = R_1^T$$

Define R_3 as

$$R_3 = [r^3_{i,j}]_{n \times n}$$

where

$$r^3_{i,j} = \begin{cases} (d_{i-1})_{n-j} & \text{for } i \leq n+1-j \\ \\ 0 & \text{for } i > n+1-j \end{cases} \qquad (129)$$

53

From Eq. 129 we can see that R_3 has the form

$$R_3 = \begin{bmatrix} (d_0)_{n-1} & (d_0)_{n-2} & \cdots & (d_0)_1 & (d_0)_0 \\ (d_1)_{n-1} & (d_1)_{n-2} & \cdots & (d_1)_1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ (d_{n-2})_{n-1} & (d_{n-2})_{n-2} & \cdots & 0 & 0 \\ (d_{n-1})_{n-1} & 0 & \cdots & 0 & 0 \end{bmatrix} \qquad (130)$$

It is shown in Appendix B that

$$R_3 = R_2 \, I^*$$

and that

$$R_3^{-1} = [p_{i,j}]_{n \times n} = R_3 \text{ rotated } 180^{\circ}$$

where

$$p_{i,j} = \begin{cases} (d_{n-i})_{j-1} & \text{for } j \geq n+1-i \\ \\ 0 & \text{for } j < n+1-i \end{cases} \qquad (131)$$

In other words, R_3^{-1} has the form

$$R_3^{-1} = \begin{bmatrix} 0 & 0 & \cdots & 0 & (d_{n-1})_{n-1} \\ 0 & 0 & \cdots & (d_{n-2})_{n-2} & (d_{n-2})_{n-2} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & (d_1)_1 & \cdots & (d_1)_{n-2} & (d_1)_{n-1} \\ (d_0)_0 & (d_0)_1 & \cdots & (d_0)_{n-2} & (d_0)_{n-1} \end{bmatrix} \qquad (132)$$

54

Define R_4 as

$$R_4 = [r^4_{i,j}]_{n \times n}$$

where

$$r^4_{i,j} = \begin{cases} (d_{j-1})_{n-i} & \text{for } j \leq n + 1 - i \\ \\ 0 & \text{for } j > n + 1 - i \end{cases} \tag{133}$$

From Eq. 133, R_4 has the form

$$R_4 = \begin{bmatrix} (d_0)_{n-1} & (d_1)_{n-1} & \cdots & (d_{n-2})_{n-1} & (d_{n-1})_{n-1} \\ (d_0)_{n-2} & (d_1)_{n-2} & \cdots & (d_{n-2})_{n-2} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ (d_0)_1 & (d_1)_1 & \cdots & 0 & 0 \\ (d_0)_0 & 0 & \cdots & 0 & 0 \end{bmatrix} \tag{134}$$

It is shown in Appendix B that

$$R_4^{-1} = [s_{i,j}]_{n \times n} = R_4 \text{ rotated } 180^{\circ}$$

where

$$s_{i,j} = \begin{cases} (d_{n-j})_{i-1} & \text{for } i \geq n + 1 - j \\ \\ 0 & \text{for } i < n + 1 - j \end{cases} \tag{135}$$

In other words, R_4^{-1} has the form

$$R_4^{-1} = \begin{bmatrix} 0 & 0 & \cdots & 0 & (d_0)_0 \\ 0 & 0 & \cdots & (d_1)_1 & (d_0)_1 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & (d_{n-2})_{n-2} & \cdots & (d_1)_{n-2} & (d_0)_{n-2} \\ (d_{n-1})_{n-1} & (d_{n-2})_{n-1} & \cdots & (d_1)_{n-1} & (d_0)_{n-1} \end{bmatrix} \tag{136}$$

The interrelationships between these equations are expressed by Eqs. 137 through 140 (see Appendix B).

$$R_1 = R_2^T = I^* \quad R_3^T = I^* \; R_4 \qquad \text{(mod-2)} \qquad (137)$$

$$R_2 = R_1^T = R_3 \quad I^* = R_4^T \; I^* \qquad \text{(mod-2)} \qquad (138)$$

$$R_3 = R_1^T \quad I^* = R_2 \quad I^* = R_4^T \qquad \text{(mod-2)} \qquad (139)$$

$$R_4 = I^* \quad R_1 = I^* \quad R_2^T = R_3^T \qquad \text{(mod-2)} \qquad (140)$$

5.4 Characteristic Polynomial and Feedback Equation

Let A be the "A" matrix for an SCRG and let A_s be the A matrix for an SSRG having the same feedback taps.

The "characteristic matrix" for the SCRG from Eq. 112 becomes

$$A + \xi I =
\begin{bmatrix}
c_1 + (\xi + 1) & c_2 & c_3 & \cdots & c_{n-2} & c_{n-1} & c_n \\
1 & (\xi + 1) & 0 & \cdots & 0 & 0 & 0 \\
0 & 1 & (\xi + 1) & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & (\xi + 1) & 0 & 0 \\
0 & 0 & 0 & \cdots & 1 & (\xi + 1) & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 & (\xi + 1)
\end{bmatrix}
\qquad (141)$$

If the substitution $\psi = \xi + 1$ is made in Eq. 141

$$A + \xi I = A_s + (\xi + 1) I = A_s + \psi I \qquad \text{(mod-2)}$$

56

using Eq. 37, the <u>characteristic polynomial for an SCRG</u> becomes

$$f(\xi) = A + \xi I \qquad (\text{mod-2})$$

$$= A_s + \psi I \qquad (\text{mod-2})$$

$$= c_0 \psi^n + c_1 \psi^{n-1} + \ldots + c_{n-1} \psi + c_n \qquad (\text{mod-2})$$

$$= c_0(\xi + 1)^n + c_1(\xi + 1)^{n-1} + \ldots + c_{n-1}(\xi + 1) + c_n \qquad (\text{mod-2}) \qquad (142)$$

where $c_0 \equiv 1$.

From Eqs. 142 and 118,

$$f(\xi) = \sum_{k=0}^{n} b_k \xi^k = \sum_{i=0}^{n} c_i(\xi + 1)^{n-i} \qquad (\text{mod-2})$$

$$= \sum_{i=0}^{n} c_i \sum_{k=0}^{n-i} (d_k)_{n-i} \xi^k \qquad (\text{mod-2}) \qquad (143)$$

Interchanging the summations in Eq. 143, we obtain

$$f(\xi) = \sum_{k=0}^{n} \left[\sum_{i=0}^{n-k} (d_k)_{n-i} c_i \right] \xi^k \qquad (\text{mod-2}) \qquad (144)$$

Equating Eqs. 7 and 144, the coefficients of the characteristic polynomial, b_i, are

$$b_k = \sum_{i=0}^{n-k} (d_k)_{n-i} c_i \qquad (\text{mod-2}) \qquad (145)$$

In matrix form, Eq. 145 becomes

$$B = R_3 C \qquad (\text{mod-2}) \qquad (146)$$

where B and C are defined to be

$$B = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_n \end{bmatrix} \qquad (147)$$

$$C = \begin{bmatrix} c_0 \\ c_1 \\ . \\ . \\ . \\ c_n \end{bmatrix} \tag{148}$$

and where R_3 is an $(n + 1) \times (n + 1)$ matrix defined in Eq. 129.

It is shown in Appendix B that R_3 is nonsingular. Therefore, from Eqs. 146 and 131

$$C = R_3^{-1} B \quad (\text{mod-2}) \tag{149}$$

where

$$R_3^{-1} = R_3 \text{ rotated } 180^o$$

From Eqs. 149 and 131

$$c_k = \sum_{i=n-k}^{n} (d_{n-k})_i \, b_i \quad (\text{mod-2}) \tag{150}$$

Given the feedback taps of an n-stage SCRG, its characteristic polynomial can be found by Eq. 145 or 146. Conversely, given any n-th degree characteristic polynomial, the feedback taps of the associated n-stage SCRG can be found by Eq. 149 or 150.

Equations 142 and 145 illustrate two important properties of SCRG's:

(1) From Eq. 142, if $c_n = 0$, then $\xi + 1$ is a factor of the characteristic polynomial $f(\xi)$; therefore, for every <u>maximal</u> <u>SCRG</u>

$$c_n = 1 \tag{151}$$

(2) Theorem 4 states that any periodic sequence from a generator with a characteristic polynomial having no constant term

58

(i. e., $b_0 = 0$) can be generated by a generator with fewer
than n stages. From Eq. 145, since $(d_0)_{n-i} = 1$

$$b_0 = \sum_{i=0}^{n} c_i \qquad (\text{mod-}2)$$

Therefore, any periodic sequence, from an SCRG for which
$\sum_{i=0}^{n} c_i = 0$ (the SCRG has an odd number of feedback taps not
counting c_0), can be generated by a generator with fewer than
n stages.

Because of Property 1, only those SCRG's will be considered for which $c_n \equiv 1$.
The feedback equation for an SCRG is defined like the feedback equation for an SSRG.

$$[n, b, \ldots, c, d, 0]_{SC}: \quad \begin{array}{l} \text{feedback equation which specifies an} \\ \text{SCRG with feedback taps } n, b, \ldots, c, \\ \text{and d closed.} \end{array} \qquad (152)$$

Note that 0 has been included in the feedback equation to indicate that $c_0 \equiv 1$, even though
there is no feedback tap from a zero stage; and, n is always present denoting $c_n = 1$. For
example, consider the six-stage SCRG with feedback taps on stages 5 and 6 shown in Fig. 12(b).
From Eqs. 146, 147, 148, and 129; C, B, and R_3 become

$$C = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \qquad (153)$$

$$R_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$B = R_3 \cdot C = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \quad (\text{mod-2}) \tag{154}$$

and from Eqs. 152, 153, and 154, the feedback equation and characteristic polynomial are

$$[6, 5, 0]_{SC} \iff (6, 4, 2, 1, 0) \tag{155}$$

Now assume a six-stage SCRG with feedback taps on Stages 1, 2, 4, and 6. R_3 is the same as above. The feedback vector C becomes

$$C = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \tag{156}$$

and from Eq. 146

$$B = R_3 C = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} \quad (\text{mod-2}) \tag{157}$$

From Eqs. 156 and 157

$$[6, 4, 2, 1, 0]_{SC} \iff (6, 5, 4, 1, 0) \tag{158}$$

Note from Eqs. 155 and 158, that, in general, the SCRG with a feedback law corresponding to the characteristic polynomial of Eq. 155 <u>does</u> <u>not</u> have a characteristic polynomial corresponding to the feedback law of Eq. 155. For the SSRG and MSRG this property is true. That is,

$$[6,5,0]_{SS} \Longleftrightarrow (6,1,0) \qquad [6,5,0]_{MS} \Longleftrightarrow (6,5,0)$$

$$[6,1,0]_{SS} \Longleftrightarrow (6,5,0) \qquad [6,5,0]_{MS} \Longleftrightarrow (6,5,0)$$

5.5 Initial Loading

As with the SSRG and the MSRG one can find the necessary initial loading for an SCRG to produce a desired n-tuple as the first n-digits generated at the last stage. The relationship for the required initial loading for the SCRG is derived below.

Through a change in time indices, Eq. 111 can be rewritten as

$$u_{i-1}(j) = u_i(j) + u_i(j+1) \qquad (\text{mod-2}) \qquad 2 \leq i \leq n \qquad (159)$$

and with $(d_0)_0 \equiv 1$,

$$u_n(j) = (d_0)_0 \, u_n(j) \qquad (160)$$

In addition, since $(d_0)_k = (d_k)_k = 1$ (see Eq. 119)

$$u_{n-1}(j) = u_n(j) + u_n(j+1) \qquad (\text{mod-2})$$

$$= (d_0)_1 \, u_n(j) + (d_1)_1 \, u_n(j+1) \qquad (\text{mod-2}) \qquad (161)$$

Assume the relationship

$$u_{n-k}(j) = \sum_{i=0}^{k} (d_i)_k \, u_n(j+i) \qquad (\text{mod-2}) \qquad (162)$$

is true for some arbitrary value of k. Then for k + 1 from Eq. 159, $k + 1 \leq n - 1$

$$u_{n-(k+1)}(j) = u_{n-k}(j) + u_{n-k}(j+1) \qquad (\text{mod-2})$$

61

$$= \sum_{i=0}^{k} (d_i)_k \ u_n(j+i) + \sum_{i=0}^{k} (d_i)_k \ u_n(j+i+1) \qquad (\text{mod-2})$$

$$= \sum_{i=0}^{k} (d_i)_k \ u_n(j+i) + \sum_{i=1}^{k+1} (d_{i-1})_k \ u_n(j+i) \qquad (\text{mod-2})$$

$$= (d_0)_k \ u_n(j) + \sum_{i=1}^{k} [(d_i)_k + (d_{i-1})k] \ u_n(j+i)$$

$$+ (d_k)_k \ u_n(j+k+1) \qquad (\text{mod-2}) \qquad (163)$$

From Eq. 119

$$(d_m)_m = (d_0)_m = 1$$

and

$$(d_i)_{k+1} = (d_i)_k + (d_{i-1})_k \qquad (\text{mod-2})$$

Thus, Eq. 163 can be written

$$u_{n-(k+1)}(j) = (d_0)_{k+1} \ u_n(j) + \sum_{i=1}^{k} (d_i)_{k+1} \ u_n(j+i) + (d_{k+1})_{k+1} \ u_n(j+k+1) \qquad (\text{mod-2})$$

$$= \sum_{i=0}^{(k+1)} (d_i)_{k+1} \ u_n(j+i) \qquad (\text{mod-2}) \qquad (164)$$

From Eqs. 160 and 161, 162 holds for $k = 0$, 1; and from Eq. 164, 162 holds for $k + 1$, k arbitrary. Thus, by induction Eq. 162 applies for $k = 0, 1, 2, \ldots, n - 1$.

Through a change in subscript, Eq. 162 becomes

$$u_k(j) = \sum_{i=0}^{n-k} (d_i)_{n-k} \ u_n(j+i) \qquad (\text{mod-2}) \qquad (165)$$

Equation 165 is the desired relationship for the initial loading $u_k(j)$ to produce at the n-th stage the n-tuple $[u_n(j), u_n(j+1), \ldots, u_n(j+n-1)]$. Equation 165 can be written in matrix form, using $U(j)$, $V_i(j)$, and R_4, defined in Eqs. 1, 15, and 133 respectively, as follows

$$U(j) = R_4 \ V_n(j) \qquad (\text{mod-2}) \qquad (166)$$

62

where

$$U(j) = \begin{bmatrix} u_1(j) \\ u_2(j) \\ . \\ . \\ . \\ u_n(j) \end{bmatrix} = \text{the required initial loading}$$

$$V_i(j) = \begin{bmatrix} u_i(j) \\ u_i(j+1) \\ . \\ . \\ . \\ u_i(j+n-1) \end{bmatrix} = \text{the desired n-tuple output}$$

and

$$R_4 = [r^4_{i,j}]_{n \times n}$$

where

$$r^4_{i,j} = (d_{j-1})_{n-i} \begin{cases} \text{for } j \leq n + 1 - i \\ \\ 0 \quad \text{for } j > n + 1 - i \end{cases}$$

Note that in Eq. 166 the initial loading for the SCRG is independent of the feedback taps of the generator. This property is also true for the SSRG.

For a given n stage SCRG, the initial loading necessary to produce a particular output n-tuple can be determined from either Eq. 165 or 166. Furthermore, it was shown in Section 5.4 that there exists an n stage SCRG associated with any n-th degree characteristic polynomial (and, hence, for any n-th degree sequence law). This results in the following theorem:

Theorem 7:

Every n stage linear sequence generator has an equivalent n stage SCRG.

63

As a special case of the above theorem, for every SSRG there is an equivalent SCRG, and vice versa. For every MSRG there is an equivalent SCRG, and vice versa.

5.6 Interstage Relationships

For every SCRG there is a matrix, H, (see Appendix B) which commutes between the output sequences produced at adjacent stages of the SCRG. In other words, if $V_i(j)$ is defined as in Eq. 15 to be an n-tuple of consecutive digits produced by the i-th stage, that is

$$V_i(j) = \begin{bmatrix} u_i(j) \\ u_i(j+1) \\ \cdot \\ \cdot \\ \cdot \\ u_i(j+n-1) \end{bmatrix}$$

then

$$H \cdot V_i(j) = V_{i-1}(j) \qquad (\text{mod-2}) \qquad 2 \leq i \leq n \qquad (167)$$

Mathematically, the matrix H is defined as

$$H = [h_{i,j}]_{n \times n}$$

where

$$\left. \begin{aligned} h_{i,i} &= 1 && \text{for } 1 \leq i \leq n-1 \\ h_{i,i+1} &= 1 && \text{for } 1 \leq i \leq n-1 \\ h_{n,i} &= b_{i-1} && \text{for } 1 \leq i \leq n-1 \\ h_{n,n} &= b_{n-1} + 1 && (\text{mod-2}) \\ h_{i,j} &= 0 && \text{otherwise} \end{aligned} \right\} \qquad (168)$$

and the b_i's are the coefficients of the characteristic polynomial associated with the SCRG. From Eq. 168, the H matrix has the form

$$H = \begin{bmatrix} 1 & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & 1 & \ldots & 0 & 0 \\ & & \vdots & & & \vdots & \\ 0 & 0 & 0 & 0 & \ldots & 1 & 1 \\ b_0 & b_1 & b_2 & b_3 & \cdots & b_{n-2} & 1+b_{n-1} \end{bmatrix} \qquad (169)$$

Furthermore, for every SCRG in which $c_n = 1$, there exists a matrix, G, (see Appendix B) such that

$$G = H^{-1} \qquad (170)$$

and thus from Eq. 167

$$G \cdot V_{i-1}(j) = V_i(j) \qquad (\text{mod-}2) \qquad 2 \leq i \leq n \qquad (171)$$

Mathematically, the matrix G is defined as

$$G = [g_{i,j}]_{n \times n}$$

where

$$\left. \begin{aligned} g_{i,j} &= 1 + \sum_{k=0}^{j-1} b_k \qquad (\text{mod-}2) \qquad \text{for } i \leq j \\ g_{i,j} &= \sum_{k=0}^{j-1} b_k \qquad (\text{mod-}2) \qquad \text{for } i > j \end{aligned} \right\} \qquad (172)$$

A complete derivation of the G and H matrices and also Eqs. 167 and 171 can be found in Appendix B.

Letting $X_i(j)$ be the sequence generated at the i-th stage of the SCRG with time reference j as defined in Section 2.2, Eq. 159 leads to the relationship

$$X_{i-1}(j) = X_i(j) + X_i(j+1) \qquad (\text{mod-}2) \qquad 2 \leq i \leq n \qquad (173)$$

which means that the sequence from the (i-1)-th stage is equal to the sequence from the i-th stage, shifted once and added to itself. Consequently, the interstage relationships of an

65

SCRG depend upon the shift-and-add property of the sequence produced. For this reason it is convenient to consider separately maximal generators, nonmaximal generators with irreducible characteristic polynomials, and nonmaximal generators with factorable characteristic polynomials.

5.6.1 Maximal SCRG. Theorem 2 states that every stage of a maximal generator produces the same sequence, but that there will be a time shift between the sequences produced by any two stages.

From Eqs. 25 and 173

$$X_{i-1}(j) = X_i(j) + X_i(j+1) \qquad (\text{mod-}2)$$

$$= X_i(j+K) \qquad (174)$$

where K is a time shift determined by the shift-and-add property of the maximal sequence. This constant, K, can be found, using the B_A matrix associated with the generator, as the solution to the equation

$$A^K = A + I \qquad (\text{mod-}2) \qquad (175)$$

where A is the "A" matrix of the SCRG. To justify the above statements, let $V_i(j)$ represent an n-tuple of the sequence $X_i(j)$. Then from Eq. 173

$$V_{i-1}(j) = V_i(j) + V_i(j+1) \qquad (\text{mod-}2) \qquad 2 \leq i \leq n \qquad (176)$$

Let K be the time shift between the sequence produced by the (i-1)-th stage and the i-th stage, that is, from Eq. 174

$$V_{i-1}(j) = V_i(j+K) \qquad (177)$$

then, from Eqs. 176, 177, and 16

$$V_{i-1}(j) = V_i(j+K) = V_i(j) + V_i(j+1) \qquad (\text{mod-}2)$$

$$= C_f^K V_i(j) = (I+C_f) V_i(j) \qquad (\text{mod-}2)$$

Thus, K is the solution to the equation

$$C_f^K = C_f + I \qquad (\text{mod-}2) \qquad (178)$$

Equation 178 is solved from the B_A matrix for the characteristic polynomial, and since the characteristic polynomial for C_f is the same as that for the A matrix of the SCRG, K can be considered as the solution to the equation

$$A^K = A + I \quad \text{(mod-2)}$$

Note that in Eq. 175 the shift for a maximal SCRG is the same for each stage since Eq. 176 is valid for all i, $2 \leq i \leq n$. As an example, consider a $[4, 3, 0]_{SC}$ maximal SCRG. Figure 13 shows this generator and its periodic maximal sequences along with the generator associated B_A matrix.

Applying Eq. 175

$$A^K = A + I \quad \text{(mod-2)}$$

or

$$K = (4)$$

Thus,

$$X_1(j) = X_2(j+4)$$
$$X_2(j) = X_3(j+4)$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$X_{n-1}(j) = X_n(j+4)$$

The shift K = 4 between each stage is verified from the sequences shown in Fig. 13.

Additional values of K are tabulated in Table 2, Section 8.4 for all maximal SCRG's of length $2 \leq n \leq 12$.

5.6.2 Nonmaximal, Irreducible Characteristic Polynomials.

In Section 2.4.1 we mentioned that when a nonmaximal generator has an irreducible characteristic polynomial all the sequences produced by the generator have the same length ℓ. Because of the partial shift-and-add property of nonmaximal generators there are certain shifts for which the shift-and-add property is exhibited, for other shifts, however, a different sequence of the same

67

The [4,3,0]_{SC} SCRG diagram with stages labeled 1_c, 2_c, 3_c, 4_c with feedback.

Time (downward):

1	0	0	0
1	0	0	0
1	1	0	0
1	0	1	0
0	1	1	1
0	1	0	0
0	1	1	0
1	1	0	1
0	0	1	1
0	0	1	0
1	0	1	1
1	1	1	0
0	0	0	1
1	0	0	1
0	1	0	1
1	1	1	1
1	0	0	0

B_A Matrix

Powers of A → 3 2 1 0

	3	2	1	0
1	0	0	1	0
2	0	1	0	0
3	1	0	0	0
4	0	0	1	1
5	0	1	1	0
6	1	1	0	0
7	1	0	1	1
8	0	1	0	1
9	1	0	1	0
10	0	1	1	1
11	1	1	1	0
12	1	1	1	1
13	1	1	0	1
14	1	0	0	1
15	0	0	0	1
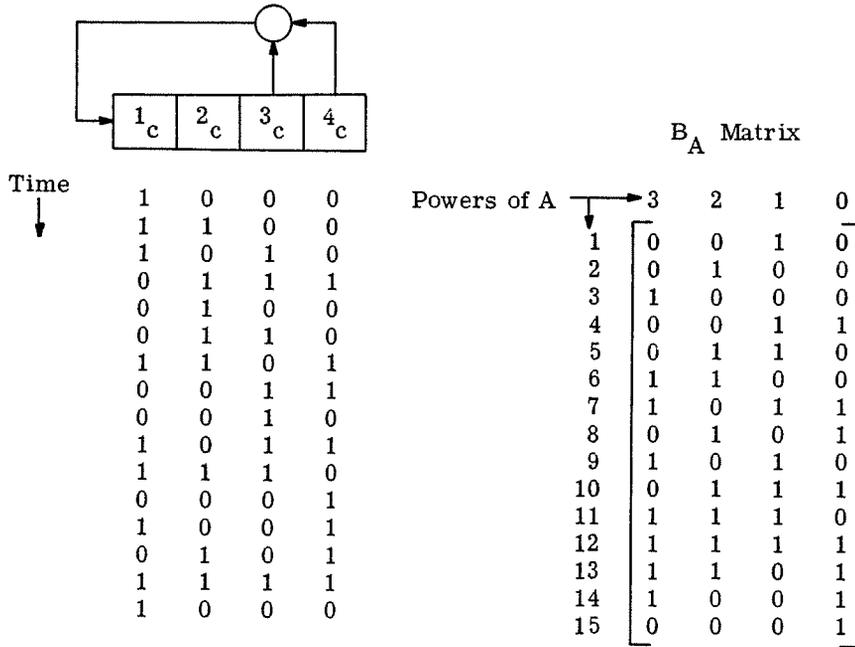
Fig. 13. The $[4,3,0]_{SC}$ SCRG, the successive content vectors, and the associated B_A matrix.

generator is obtained. Since

$$X_{i-1}(j) = X_i(j) + X_i(j+1) \qquad (\text{mod-}2)$$

if "1" is a shift for which the shift-and-add property holds, then the sequence produced by the $(i-1)$-th stage will be a shifted version of the sequence produced by the i-th stage. If, on the other hand, the shift-and-add property does not hold for a shift of "1," then the sequence produced by the $(i-1)$-th stage will be different from the sequence produced by the i-th stage. Further, if there are m different sequences, then it can be shown that when $m \leq n$, every set of m consecutive stages of the generator will produce all m of the possible sequences, and that when $m \geq n$, every stage will produce a different sequence.

5.6.3 Nonmaximal, Factorable Characteristic Polynomials. It was pointed out in Theorem 4 that any periodic sequence from a generator with a characteristic polynomial that has ξ^k as a factor can be generated by a generator with $n-k$ stages. Therefore, only generators with a characteristic polynomial that has a constant term will be considered, that

68

is, $b_0 = 1$; and since (see Eq. 145)

$$b_0 = \sum_{i=0}^{n} c_i \qquad (\text{mod-}2)$$

only those generators for which

$$\sum_{i=0}^{n} c_i = 1 \qquad (\text{mod-}2)$$

will be considered.

The conclusion follows directly from Eq. 142 that $(\xi + 1)^k$ is a factor of $f(\xi)$, if and only if, $c_i = 0$ for $i > n - k$. For these generators, Eqs. 167 and 173 hold, but the G matrix is not defined so that Eq. 171 does not hold.

For all the remaining SCRG's, $c_n = 1$ and $\sum_{i=0}^{n} c_i = 1$. For these generators the matrices H and G exist and the following theorems apply.

Theorem 8:

Consider an n-stage SCRG, for which $c_n = 1$, and $\sum_{i=0}^{n} c_i = 1$, with a characteristic polynomial, $f(\xi)$, which is factorable. If any stage of the SCRG is producing a sequence corresponding to a polynomial of degree less than n, $f'(\xi)$, where $f(\xi) = f''(\xi) \cdot f'(\xi)$, then the sequences from every stage of the generator correspond to the same polynomial $f'(\xi)$.

Theorem 9:

Consider an n-stage SCRG with $c_n = 1$ and $\sum_{i=0}^{n} c_i = 1$, with a characteristic polynomial, $f(\xi)$, which is factorable, $f(\xi) = f'(\xi) \ldots f''(\xi)$. If any p consecutive stages of the generator $(p \leq n)$ contain zeros at any time j, then none of the sequences being produced by the generator can be produced by a generator of p or fewer stages, unless every stage is producing all zeros.

Both Theorems 8 and 9 are proved in Appendix B.

As an application of Theorems 8 and 9, consider the eight-stage SCRG with feedback law and characteristic equation

$$[8,6,5,4,3,2,0]_{SC} \Longleftrightarrow (8,6,5,4,3,2,0) = (3,1,0)(3,2,0)(2,1,0) = (6,5,4,3,2,1,0)(2,1,0)$$

We discussed in Section 2.4.2 that the sequences of a $(3,1,0)$ generator, a $(3,2,0)$ generator, and a $(2,1,0)$ can be produced by an $(8,6,5,4,3,2,0)$ generator. Theorem 8 states that if any stage is generating a sequence which follows, for example, the $(6,5,4,3,2,1,0)$ sequence law and not a law of degree less than 6, then every stage is generating a sequence that follows this sequence law. Consequently, no stage will be generating a sequence corresponding to any of the irreducible factors. On the other hand if, for example, any stage of the generator is generating the $(3,1,0)$ sequence then every stage is generating the $(3,1,0)$ sequence. No stage is generating a sequence corresponding to $(3,2,0)$ or $(2,1,0)$. Theorem 9 states that if the SCRG is initially loaded with a content vector containing at least three consecutive zeros, such as

$$U(0) = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \quad \text{or} \quad U(0) = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad \text{or} \quad U(0) = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

then the generator cannot produce the $(3,1,0)$ sequence, the $(3,2,0)$ sequence, or the $(2,1,0)$ sequence.

A consequence of Theorem 8 is that if one stage of the SCRG is producing a sequence that corresponds to an irreducible factor of the characteristic polynomial, then every stage is producing a sequence that corresponds to the same factor. The interstage relationships found in Sections 5.6.1 and 5.6.2 for maximal and irreducible nonmaximal sequences are true if the specific factor involved is taken to be the characteristic polynomial.

5.7 Output Adder Circuit

An output adder circuit can be used with the SCRG to generate a shifted version of the same sequence or a new sequence in a manner similar to the adder for the SSRG and MSRG. Figure 14 shows an SCRG with an output adder.
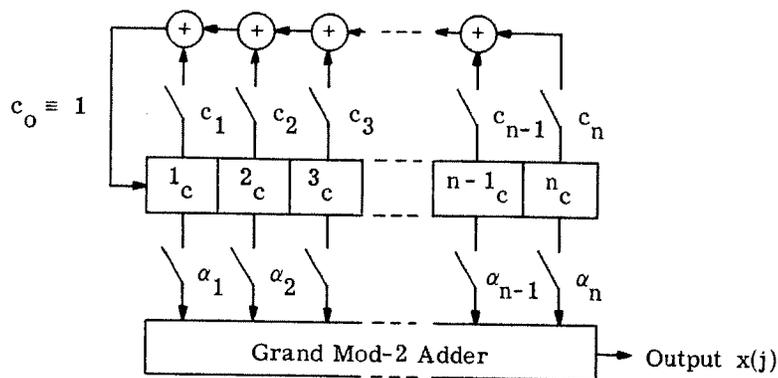
Fig. 14. An SCRG with an output adder circuit.

Let $\bar{\alpha}$, $X(j)$, F_A, and R_2 be defined as in Eqs. 52, 51, 59, and 126, that is

$$\bar{\alpha} = [\alpha_1, \ldots, \alpha_n]$$

where

α_i = 1 if the i-th adder in Fig. 13 is closed

= 0 if the i-th adder in Fig. 13 is open

$X(j) = [x(j), \ldots, x(j+n-1)]$

= the initial n-tuple of output digits desired from the adder, when $U(j) = E_1(0)$

$$F_A = [f_{i,j}]_{n \times n}$$

where

$$f_{i,j} = c_{j-i} \quad \text{for } i \leq j$$

$$= 0 \quad \text{for } i > j$$

and

$$R_2 = [r^2_{i,j}]_{n \times n}$$

where

$$r^2_{i,j} = (d_{i-1})_{j-1} \quad \text{for } i \leq j$$

$$= 0 \quad \text{for } i > j$$

71

Then

$$\bar{\alpha} = X(j) \cdot R_2 \, F_A \qquad (\text{mod-2}) \qquad (179)$$

or, expressed in series form

$$\alpha_i = \sum_{m=1}^{i} \left[\sum_{k=0}^{i-m} (d_{m-1})_{i-1-k} \, c_k \right] x(j+m-1) \qquad (\text{mod-2}) \qquad (180)$$

The derivation of Eqs. 179 and 180 requires the following theorem which is proved in Appendix B.

Theorem 10:

Consider an n-stage SSRG and an n-stage SCRG which have the same feedback (not characteristic) equation. Let Y(j) represent the content vector of the SSRG at time j, and let U(j) represent the content vector of the SCRG at time j. If U(K) = Y(K) at some time K, then

$$[U(K), U(K+1), \ldots, U(K+n-1)] = [Y(K), Y(K+1), \ldots, Y(K+n-1)] \cdot R_2 \qquad (\text{mod-2}) \qquad (181)$$

and

$$[Y(K), Y(K+1), \ldots, Y(K+n-1)] = [U(K), U(K+1), \ldots, U(K+n-1)] \cdot R_2 \qquad (\text{mod-2}) \qquad (182)$$

Returning to the derivation of Eq. 179, let U(j) be the content vector of the SCRG in Fig. 14. Then the output of the adder at time j is

$$x(j) = \sum_{i=1}^{n} \alpha_i \, u_i(j) \qquad (\text{mod-2})$$

or

$$x(j) = \bar{\alpha} \cdot U(j) \qquad (\text{mod-2})$$

and

$$X(j) = [\bar{\alpha} \cdot U(j), \bar{\alpha} \cdot U(j+1), \ldots, \bar{\alpha} \cdot U(j+n-1)] \qquad (\text{mod-2})$$

$$= \bar{\alpha} \cdot [U(j), U(j+1), \ldots, U(j+n-1)] \qquad (\text{mod-2}) \qquad (183)$$

Consider an SSRG with the _same feedback equation_ as the SCRG, let $Y(j)$ represent the content vector of the SSRG at time j, and let

$$Y(j) = E_1(0) = \begin{bmatrix} 1 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix}$$

Then for the SSRG, from Eq. 58

$$[Y(j), Y(j+1), \ldots, Y(j+n-1)] = [E_1(0), E_1(1), \ldots, E_1(n-1)]$$

$$= E_A \tag{184}$$

and from Eqs. 60 and 59

$$E_A^{-1} = F_A$$

where

$$F_A = [f_{i,j}]_{n \times n}$$

$$f_{i,j} = c_{j-i} \qquad i \leq j$$

$$= 0 \qquad i > j$$

If the SCRG is initially loaded at time j with

$$U(j) = E_1(0)$$

then

$$U(j) = Y(j)$$

and from Eq. 181 and 184

$$[U(j), U(j+1), \ldots, U(j+n-1)] = [Y(j), Y(j+1), \ldots, Y(j+n-1)] \cdot R_2 \qquad (\text{mod-2})$$

$$= E_A \cdot R_2 \qquad (\text{mod-2}) \tag{185}$$

73

Using Eqs. 183, 185, 128, and 60

$$X(j) = \bar{\alpha} \cdot E_A \cdot R_2 \qquad (\text{mod-2})$$

and

$$\bar{\alpha} = X(j) \cdot R_2^{-1} \cdot E_A^{-1} \qquad (\text{mod-2})$$

$$= X(j) \cdot R_2 \cdot F_A \qquad (\text{mod-2}) \qquad (179)$$

In series form,

$$R_2 \cdot F_A = [r_{i,j}^2] \cdot [f_{i,j}] = [p_{i,j}] \qquad (\text{mod-2})$$

where

$$p_{i,j} = \sum_{k=1}^{n} r_{i,k}^2 \cdot f_{k,j} \qquad (\text{mod-2})$$

$$= \sum_{k=i}^{j} (d_{i-1})_{k-1} \, c_{j-k} \qquad (\text{mod-2}) \quad \text{for } i \leq j$$

$$= 0 \qquad (\text{mod-2}) \quad \text{for } i > j$$

then letting $x_i = x(j+i-1)$

$$[\alpha_i] = [x_i] \cdot [p_{i,j}] \qquad (\text{mod-2})$$

$$\alpha_i = \sum_{m=1}^{n} x_m \, p_{m,i} \qquad (\text{mod-2})$$

$$= \sum_{m=1}^{i} x_m \sum_{k=m}^{i} (d_{m-1})_{k-1} \, c_{i-k} \qquad (\text{mod-2})$$

$$\alpha_i = \sum_{m=1}^{i} \left[\sum_{k=0}^{i-m} (d_{m-1})_{i-1-k} \, c_k \right] x(j+m-1) \qquad (\text{mod-2}) \qquad (180)$$

Either Eq. 179 or 180 can be used to find the proper adder taps to close to get

$x(j), \ldots, x(j+n-1)$ as the initial output of the adder when the elementary load $E_1(0)$ is

present in the generator.

74

6. THE MODULAR COMPLEMENT-REGISTER GENERATOR

In Section 5 we discussed the fact that a linear-sequence generator can be constructed by replacing the shift stages of an SSRG by complement stages. Similarly, another type of linear-sequence generator can be constructed by replacing the shift stages of an MSRG by complement stages. The resulting generator becomes a "modular complement register generator" (MCRG), and is the subject of this section. The MCRG is developed in a manner parallel to the development of the MSRG.

6.1 Definition

The general form of the modular complement register is shown in Fig. 15(a).

The operation of the MCRG is similar to the operation of the MSRG. Every stage (except the first) is fed by the previous stage and by the n-th stage if the feedback tap preceding that stage is closed. The c_i's in Fig. 15 represent the feedback taps,

$$
\left.
\begin{aligned}
c_i &= 1 \text{ if the n-th stage feeds the } i+1\text{-th stage} \\
&= 0 \text{ if the n-th stage does not feed the } i+1\text{-th stage} \\
c_n &\equiv 1
\end{aligned}
\right\} \tag{186}
$$

6.2 The A Matrix

From Section 2.1 the A matrix is defined by the following relation

$$ A = [a_{i,j}]_{n \times n} $$

where

$$
\begin{aligned}
a_{i,j} &= 1 \text{ if the j-th stage of the generator feeds the i-th stage} \\
&= 0 \text{ otherwise.}
\end{aligned}
$$

It is obvious from Fig. 15 for the MCRG and from Fig. 10 for the equivalent operation of a complement stage that the content of the i-th stage at time j is given by

(a)

(b)
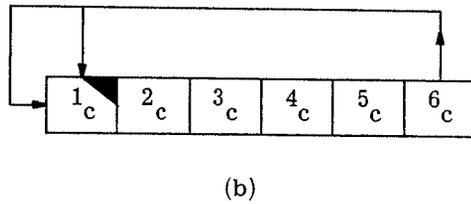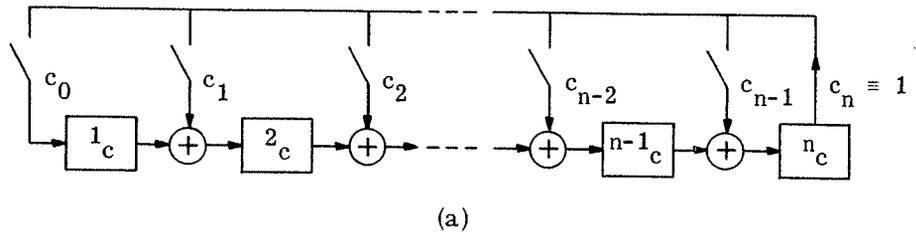
Fig. 15. An n-stage MCRG, (a) general representation,
(b) schematic representation of a six-stage MCRG
with feedback taps c_1 and c_0 closed.

$$u_1(j) = u_1(j-1) + c_0 u_n(j-1) \qquad \text{(mod-2)}$$

$$u_i(j) = u_i(j-1) + u_{i-1}(j-1) + c_{i-1} u_n(j-1) \quad \text{(mod-2)} \qquad 2 \leq i \leq n$$

$$\left. \right\} \quad (187)$$

Thus, for the MCRG the A matrix becomes

$$A = [a_{i,j}]_{n \times n}$$

where

$$a_{i,i} = 1 \qquad \text{for} \quad 1 \leq i \leq n-1$$

$$a_{i+1,i} = 1 \qquad \text{for} \quad 1 \leq i \leq n-1$$

$$a_{i,n} = c_{i-1} \qquad \text{for} \quad 1 \leq i \leq n-1$$

$$a_{n,n} = 1 + c_{n-1} \qquad \text{(mod-2)}$$

$$a_{i,j} = 0 \qquad \text{otherwise}$$

$$\left. \right\} \quad (188)$$

that is, the A matrix for the MCRG has the form

76

$$A = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & c_0 \\ 1 & 1 & 0 & \cdots & 0 & 0 & c_1 \\ 0 & 1 & 1 & \cdots & 0 & 0 & c_2 \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 & 1 & c_{n-2} \\ 0 & 0 & 0 & \cdots & 0 & 1 & (1+c_{n-1}) \end{bmatrix} \qquad (189)$$

6.3 Characteristic Polynomial and Feedback Equation

Let A be the "A" matrix for an MCRG and let A_m be the A matrix for the MSRG which has the same feedback taps. A comparison of Eqs. 65 and 189 shows that

$$A = A_m + I \qquad (\text{mod-2}) \qquad (190)$$

By comparison with Eq. 68, the characteristic polynomial for the MCRG becomes

$$f(\xi) = \sum_{k=0}^{n} b_k \, \xi^k \qquad (\text{mod-2})$$

$$= |A + \xi I| \qquad (\text{mod-2})$$

$$= |A_m + (\xi+1) I| \qquad (\text{mod-2})$$

$$= \sum_{i=0}^{n} c_i (\xi+1)^i = \sum_{i=0}^{n} c_i \sum_{k=0}^{i} (d_k)_i \, \xi^k \qquad (\text{mod-2}) \qquad (191)$$

Interchanging the summations in Eq. 191, the characteristic polynomial for an MCRG becomes

$$f(\xi) = \sum_{k=0}^{n} \left[\sum_{i=k}^{n} (d_k)_i \, c_i \right] \xi^k \qquad (\text{mod-2}) \qquad (192)$$

and the coefficients of the characteristic polynomial, b_k, become

$$b_k = \sum_{i=k}^{n} (d_k)_i \, c_i \qquad (\text{mod-2}) \qquad (193)$$

Defining the column vectors B and C as in Eqs. 147 and 148, Eq. 193 in matrix

77

form becomes

$$B = R_2 \cdot C \quad (\text{mod-2}) \tag{194}$$

where

$$B = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_n \end{bmatrix} \qquad C = \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{bmatrix}$$

and where R_2 is an $(n+1) \times (n+1)$ matrix defined in Eq. 126. Furthermore, since R_2 is an involuntary matrix $(R_2^{-1} = R_2)$

$$C = R_2 \cdot B \quad (\text{mod-2}) \tag{195}$$

which can be written

$$c_k = \sum_{i=k}^{n} (d_k)_i \, b_i \quad (\text{mod-2}) \tag{196}$$

Given the feedback taps of an n-stage MCRG, its characteristic polynomial can be found by either Eq. 194 or 193. Conversely, given any n-th degree characteristic polynomial the feedback taps of the associated n-stage MCRG can be found by either Eq. 195 or 196.

Equations 191 and 193 illustrate two important properties of MCRG's:

1. From Eq. 191, if $c_0 = 0$, then $(\xi + 1)$ is a factor of $f(\xi)$; therefore, for every <u>maximal MCRG</u>, $c_0 = 1$. (197)

2. From Eq. 193, since $(d_0)_i = 1$,

$$b_0 = \sum_{i=0}^{n} c_i \quad (\text{mod-2})$$

Therefore, applying Theorem 4, any periodic sequence from an n-stage MCRG for which $\sum_{i=0}^{n} c_i = 0$ (the MCRG has an odd number of feedback taps, not counting c_n) can be generated by a generator having fewer than n-stages.

78

Because of Property 1 the convention $c_o = c_n \equiv 1$ will be made for this report. The feedback equation for an MCRG is defined in the same way as the feedback equation for an SSRG.

$$[n, a, b, \ldots, c, 0]_{MC} : \quad \underline{\text{feedback equation}} \text{ which specifies an MCRG with feedback taps } a, b, \ldots, c, 0 \text{ closed.} \qquad (198)$$

Note that n has been included in the feedback equation to indicate that $c_n \equiv 1$ even though there is no feedback to an $n+1$-th stage, and 0 is always present denoting $c_o = 1$.

For example, to find the characteristic polynomial of the $[6, 1, 0]_{MC}$ MCRG shown in Fig. 15(b), Eq. 194 is used,

$$B = R_2 \cdot C \qquad (\text{mod-2})$$

$$B = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \qquad (\text{mod-2})$$

That is,

$$[6, 1, 0]_{MC} \Longleftrightarrow (6, 4, 2, 1, 0)$$

Note that by comparison of this example with the example of Page 60, for the same characteristic polynomial, the MCRG and SCRG feedback equations are simple reverses. This property is also exhibited by the SSRG and the MSRG.

Formally, from Eqs. 196 and 150 repeated below

$$c_k = \sum_{i=k}^{n} (d_k)_i \, b_i \qquad (\text{mod-2}) \quad \text{for} \quad \text{MCRG} \qquad (196)$$

$$c_k' = \sum_{i=n-k}^{n} (d_{n-k})_i \, b_i \qquad (\text{mod-2}) \quad \text{for} \quad \text{SCRG} \qquad (150)$$

79

Replacing k by $n-k$ in Eq. 196 and equating, one obtains

$$c_{n-k} = c_k'$$

or, in other words, the feedback taps are a simple reverse if the characteristic polynomial is identical (b_i).

6.4 Initial Loading

Like the SSRG, the MSRG, and the SCRG, it is possible to find the required initial loading of the MCRG to produce a desired n-tuple as the first n output digits of the last stage of the generator. It follows that by proper loading, every sequence which obeys the sequence law of the generator can be obtained from the last stage.

Let $u_n(j), \ldots, u_n(j+n-1)$ be the desired initial n-tuple from the last stage starting at time j, and let c_i represent the feedback taps of the MCRG. Then the initial loading of the generator at time j is given by the following equation:

$$u_p(j) = \sum_{m=0}^{n-p} \left[\sum_{k=p+m}^{n} (d_m)_{k-p} c_k \right] u_n(j+m) \quad \text{(mod-2)} \tag{199}$$

In matrix form Eq. 199 can be written

$$U(j) = F_M \cdot R_1 \cdot V_n(j) \quad \text{(mod-2)} \tag{200}$$

where $U(j)$, $V_i(j)$, R_1, and F_M are defined as in Eqs. 1, 15, 123, and 79.

The derivation of Eqs. 199 and 200 proceeds as follows: Equation 187 can be written

$$u_{i-1}(j) = u_i(j) + u_i(j+1) + c_{i-1} u_n(j) \quad \text{(mod-2)} \quad 2 \leq i \leq n \tag{201}$$

With $c_n \equiv 1$, and by definition $(d_o)_i \equiv (d_i)_i \equiv 1$.

$$u_n(j) = u_n(j)$$

$$= (d_o)_o c_n u_n(j) \tag{202}$$

and

$$u_{n-1}(j) = u_n(j) + u_n(j+1) + c_{n-1} u_n(j) \quad (\text{mod-2})$$

$$= [(d_0)_1 c_n + (d_0)_0 c_{n-1}] u_n(j) + (d_1)_1 c_n u_n(j+1) \quad (\text{mod-2}) \tag{203}$$

Assume that for some particular integer k, where $1 \leq k \leq n-2$, the following equation holds:

$$u_{n-k}(j) = \sum_{m=0}^{k} \left[\sum_{i=0}^{m} (d_{k-m})_{k-i} c_{n-i} \right] u_n(j+k-m) \quad (\text{mod-2}) \tag{204}$$

Then using Eqs. 201, 204, and 119

$$u_{n-(k+1)}(j) = u_{n-k}(j) + u_{n-k}(j+1) + c_{n-(k+1)} u_n(j) \quad (\text{mod-2})$$

$$= \sum_{m=0}^{k} \left[\sum_{i=0}^{m} (d_{k-m})_{k-i} c_{n-i} \right] u_n(j+k-m)$$

$$+ \sum_{m=0}^{k} \left[\sum_{i=0}^{m} (d_{k-m})_{k-i} c_{n-i} \right] u_n(j+k+1-m) + c_{n-(k+1)} u_n(j) \quad (\text{mod-2})$$

$$= \underbrace{\sum_{m=0}^{k-1} \left[\sum_{i=0}^{m} (d_{k-m})_{k-i} c_{n-i} \right] u_n(j+k-m)}_{\textcircled{1}} + \underbrace{\left[\sum_{i=0}^{k} (d_0)_{k-i} c_{n-i} \right] u_n(j)}_{\textcircled{2}}$$

$$+ \underbrace{\sum_{m=1}^{k} \left[\sum_{i=0}^{m-1} (d_{k-m})_{k-i} c_{n-i} \right] u_n(j+k+1-m)}_{\textcircled{3}}$$

$$+ \underbrace{\sum_{m=0}^{k} (d_{k-m})_{k-m} c_{n-m} u_n(j+k+1-m)}_{\textcircled{4}} + \underbrace{c_{n-(k+1)} u_n(j)}_{\textcircled{5}} \quad (\text{mod-2})$$

81

By reindexing, $\textcircled{1}$ becomes

$$\sum_{m=1}^{k} \left[\sum_{i=0}^{m-1} (d_{k+1-m})_{k-i} \, c_{n-i} \right] u_n(j+k+1-m) \quad (\text{mod-2}) \tag{205}$$

Combining Eq. 205 and $\textcircled{3}$ and using $(d_i)_{k+1} = (d_i)_k + (d_{i-1})_k$, one obtains

$$\sum_{m=1}^{k} \left[\sum_{i=0}^{m-1} (d_{k+1-m})_{k+1-i} \, c_{n-i} \right] u_n(j+k+1-m) \quad (\text{mod-2}) \tag{206}$$

Using the relation $(d_0)_k = (d_0)_{k+1} = 1$, $\textcircled{2}$ becomes

$$\left[\sum_{i=0}^{k} (d_0)_{k+1-i} \, c_{n-i} \right] u_n(j) \quad (\text{mod-2}) \tag{207}$$

Equations 206 and 207 combine to give

$$\sum_{m=1}^{k+1} \left[\sum_{i=0}^{m-1} (d_{k+1-m})_{k+1-i} \, c_{n-i} \right] u_n(j+k+1-m) \quad (\text{mod-2}) \tag{208}$$

Using the relationship $(d_{k-m})_{k-m} = (d_{k+1-m})_{k+1-m} = 1$, $\textcircled{4}$ can be written

$$\sum_{m=0}^{k} (d_{k+1-m})_{k+1-m} \, c_{n-m} \, u_n(j+k+1-m) \quad (\text{mod-2}) \tag{209}$$

and then combining Eq. 209 with $\textcircled{5}$ one gets

$$\sum_{m=0}^{k+1} (d_{k+1-m})_{k+1-m} \, c_{n-m} \, u_n(j+k+1-m) \quad (\text{mod-2}) \tag{210}$$

Then combining Eq. 208 and 210 one obtains the result

$$u_{n-(k+1)}(j) = \sum_{m=0}^{k+1} \left[\sum_{i=0}^{m} (d_{k+1-m})_{k+1-i} \, c_{n-i} \right] u_n(j+k+1-m) \quad (\text{mod-2}) \tag{211}$$

Equation 204 reduces to Eqs. 202 and 203 when $k = 0$ and $k = 1$, respectively. Equation 211 shows that if Eq. 204 is true for a particular value of k where $1 \le k \le n-2$, then it is true for the next higher value of k. Thus, by induction, Eq. 204 holds for

82

$0 \leq k \leq n-1.$

Letting $p = n-k$, Eq. 204 becomes

$$u_p(j) = \sum_{r=0}^{n-p} \left[\sum_{i=0}^{r} (d_{n-p-r})_{n-p-i} \, c_{n-i} \right] u_n(j+n-p-r) \quad (\text{mod-2}) \tag{212}$$

then letting $m = n-p-r$, Eq. 212 can be written as

$$u_p(j) = \sum_{m=0}^{n-p} \left[\sum_{i=0}^{n-p-m} (d_m)_{n-p-i} \, c_{n-i} \right] u_n(j+m) \quad (\text{mod-2}) \tag{213}$$

and letting $k = n-i$, Eq. 213 becomes

$$u_p(j) = \sum_{m=0}^{n-p} \left[\sum_{k=p+m}^{n} (d_m)_{k-p} \, c_k \right] u_n(j+m) \quad (\text{mod-2}) \tag{199}$$

Equation 200 is simply Eq. 199 written in matrix form and follows from inspection. For example, suppose the n-tuple $V_n(j)^T = [1\ 0\ 1\ 1\ 0]$ is desired as the first five digits from the last stage of a five stage MCRG with the feedback law and associated characteristic polynomial

$$[5,3,0]_{MC} \iff (5,4,3,2,0)$$

Applying Eq. 200

$$U(j) = F_M \cdot R_1 \cdot V_n(j)$$

$$U(j) = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \quad (\text{mod-2})$$

$$= \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} \quad (\text{mod-2})$$
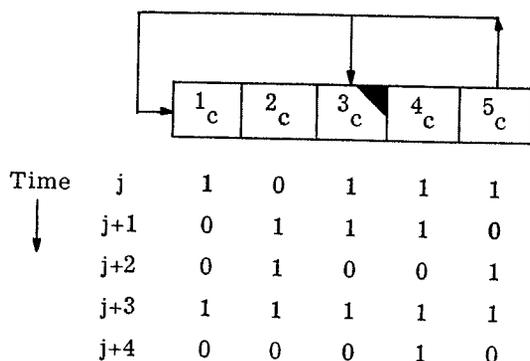
Fig. 16. A $[5,3,0]_{MC}$ MCRG and the first five content vectors for the initial loading $U(j)^T = [1,0,1,1,1]$.

The first n content vectors of a $[5,3,0]_{MC}$ MCRG beginning with the initial loading $U(j)^T = [1\ 0\ 1\ 1\ 1]$ is shown in Fig. 16. The desired output n-tuple is generated at the last stage of the generator.

6.5 Interstage Relationships

Equation 187 can be rewritten as

$$u_i(j) = u_{i+1}(j) + u_{i+1}(j+1) + c_i\, u_n(j) \qquad (\text{mod-2}) \qquad (214)$$

Letting $X_i(j)$ represent the sequence produced by the i-th stage with time reference j, and applying the definition of sequence addition from Section 2.2, the following relationship results:

$$X_i(j) = X_{i+1}(j) + X_{i+1}(j+1) + c_i\, X_n(j) \qquad (\text{mod-2}) \qquad (215)$$

Equation 215 is a general relationship for any MCRG. Since the interstage sequence relationships depend on the shift-and-add properties of the sequence produced, it is convenient to individually consider maximal generators, nonmaximal generators with irreducible characteristic polynomials, and nonmaximal generators with factorable characteristic polynomials.

6.5.1 Maximal MCRG. Theorem 2 states that every stage of a maximal MCRG produces the same sequence, but the sequence from each stage will be shifted in time from the sequence from every other stage. If two adjacent stages are not separated by an interstage mod-2 adder, $c_i = 0$, Eq. 215 reduces to

84

$$X_i(j) = X_{i+1}(j) + X_{i+1}(j+1) \quad \text{(mod-2)} \tag{216}$$

This is the same relationship that exists between adjacent stages of a maximal SCRG, which is, from the shift-and-add property of maximal sequences,

$$X_i(j) = X_{i+1}(j+K) \tag{217}$$

where K is a time shift determined by the solution of the equation

$$A^K = A + I \quad \text{(mod-2)}$$

where A is the "A" matrix for the MCRG.

When two adjacent stages are separated by an adder, $c_i = 1$, Eq. 215 becomes

$$X_i(j) = X_{i+1}(j) + X_{i+1}(j+1) + X_n(j) \quad \text{(mod-2)}$$

Let $J_{i,k}$ be the time shift between the sequences produced by the i-th and k-th stages so that

$$X_i(j) = X_k(j + J_{i,k})$$

and

$$X_i(j) = X_{i+1}(j + J_{i,i+1})$$

The following discussion develops one method for determining the shift $J_{i,n}$ between the i-th stage and the n-th stage:

From Eq. 16

$$V_i(j+k) = C_f^k V_i(j) \quad \text{(mod-2)}$$

where C_f is the companion matrix for the characteristic polynomial of the generator and $V_i(j)$ is an n-tuple of digits from the i-th stage of the MCRG with time reference j,

$$V_i(j) = \begin{bmatrix} u_i(j) \\ u_i(j+1) \\ \cdot \\ \cdot \\ \cdot \\ u_i(j+n-1) \end{bmatrix}$$

It follows from Eq. 214 that

$$V_i(j) = V_{i+1}(j) + V_{i+1}(j+1) + c_i \, V_n(j) \quad \text{(mod-2)}$$

Letting $J_{i,n}$ be the shift between the sequence from the i-th stage and the sequence from the n-th stage,

$$V_i(j) = V_n(j + J_{i,n})$$

Then

$$V_{n-1}(j) = V_n(j + J_{n-1,n})$$

$$= C_f^{J_{n-1,n}} \, V_n(j) \quad \text{(mod-2)}$$

$$= V_n(j) + V_n(j+1) + c_{n-1} \, V_n(j) \quad \text{(mod-2)}$$

$$= (C_f + I + c_{n-1} \, I) \, V_n(j) \quad \text{(mod-2)} \tag{218}$$

and

$$C_f^{J_{n-1,n}} = c_n(C_f + I) + c_{n-1} \, I \quad \text{(mod-2)} \tag{219}$$

where $c_n \equiv 1$.
Similarly,

$$V_{n-2}(j) = V_n(j + J_{n-2,n})$$

$$= C_f^{J_{n-2,n}} \, V_n(j) \quad \text{(mod-2)}$$

$$= V_{n-1}(j) + V_{n-1}(j+1) + c_{n-2} \, V_n(j) \quad \text{(mod-2)}$$

$$= (C_f + I) \, V_{n-1}(j) + c_{n-2} \, V_n(j) \quad \text{(mod-2)}$$

using Eq. 218

$$V_{n-2}(j) = (C_f + I) [c_n(C_f + I) + c_{n-1} I] V_n(j) + c_{n-2} V_n(j) \quad (mod-2)$$

$$= [c_n(C_f + I)^2 + c_{n-1}(C_f + I) + c_{n-2} I] V_n(j) \quad (mod-2)$$

and

$$C_f^{J_{n-2,n}} = c_n(C_f + I)^2 + c_{n-1}(C_f + I) + c_{n-2} I \quad (mod-2) \qquad (220)$$

Assume for some arbitrary value of i, $1 \leq i \leq n-2$ that

$$C_f^{J_{n-i,n}} = c_n(C_f + I)^i + c_{n-1}(C_f + I)^{i-1} + \ldots + c_{n-i} I \quad (mod-2) \qquad (221)$$

then for the n-i-1st stage

$$V_{n-i-1}(j) = V_n(j + J_{n-i-1,n})$$

$$= C_f^{J_{n-i-1,n}} V_n(j) \quad (mod-2)$$

$$= V_{n-i}(j) + V_{n-i}(j+1) + c_{n-i-1} V_n(j) \quad (mod-2)$$

$$= (C_f + I) V_{n-i}(j) + c_{n-i-1} V_n(j) \quad (mod-2)$$

$$= (C_f + I) [c_n(C_f + I)^i + c_{n-1}(C_f + I)^{i-1} + \ldots + c_{n-i} I] V_n(j) + c_{n-i-1} V_n(j) \quad (mod-2)$$

$$= [c_n(C_f + I)^{i+1} + c_{n-1}(C_f + I)^i + \ldots + c_{n-i}(C_f + I) + c_{n-i-1} I] V_n(j) \quad (mod-2)$$

and

$$C_f^{J_{n-i-1,n}} = c_n(C_f + I)^{i+1} + c_{n-1}(C_f + I)^i + \ldots + c_{n-i}(C_f + I) + c_{n-i-1} I \quad (mod-2) \qquad (222)$$

Equation 222 shows that if Eq. 221 is true for some arbitrary value of i, then it is true for

the next larger value of i. Equations 219 and 220 show that Eq. 221 is true for i = 1 and

i = 2; thus by induction Eq. 221 is true for $1 \leq i \leq n-1$. Equation 221 can be solved for

$J_{n-i,n}$ by use of the B_A matrix associated with the characteristic polynomial. However,

since C_f and the A matrix for the MCRG have the same characteristic polynomial they also have the same B_A matrix and $J_{n-i, n}$ can be considered to be the solution to the equation

$$A^{J_{n-i, n}} = \sum_{k=0}^{i} c_{n-k}(A + I)^{i-k} \quad (\text{mod-2}) \tag{223}$$

which can be solved for $J_{n-i, n}$ using the associated B_A matrix.

As an example, consider the $[4, 1, 0]_{MC}$ MCRG which has the characteristic polynomial $(4, 1, 0)$. Figure 17 shows this generator, its output for one period, and its associated B_A matrix. For the MCRG in Fig. 17, using Eq. 223

$$A^{J_{3, 4}} = c_4(A + I) + c_3 I \quad (\text{mod-2})$$

$$= A + I \quad (\text{mod-2})$$

$$A^{J_{2, 4}} = c_4(A + I)^2 + c_3(A + I) + c_2 I \quad (\text{mod-2})$$

$$= A^2 + I \quad (\text{mod-2})$$

$$A^{J_{1, 4}} = c_4(A + I)^3 + c_3(A + I)^2 + c_2(A + I) + c_1 I \quad (\text{mod-2})$$

$$= A^3 + A^2 + A + I + I \quad (\text{mod-2})$$

$$= A^3 + A^2 + A \quad (\text{mod-2})$$

and from the B_A matrix

$$J_{1, 4} = 11$$

$$J_{2, 4} = 8$$

$$J_{3, 4} = 4$$

which means that

$$X_1(j) = X_4(j + 11)$$

$$X_2(j) = X_4(j + 8)$$

$$X_3(j) = X_4(j + 4)$$

88

which can be readily verified from the sequences shown in Fig. 17.

Using Eqs. 91 and 92, the shift between stages of the MCRG in Fig. 17 is found
to be

$$J_{1,2} = 3$$

$$J_{2,3} = 4$$

$$J_{3,4} = 4$$

or

$$X_1(j) = X_2(j + 3)$$

$$X_2(j) = X_3(j + 4)$$

$$X_3(j) = X_4(j + 4)$$

The shift between sequences not separated by an adder is the same, as pre-
dicted by Eq. 217. The shift between sequences separated by an interstage adder is some

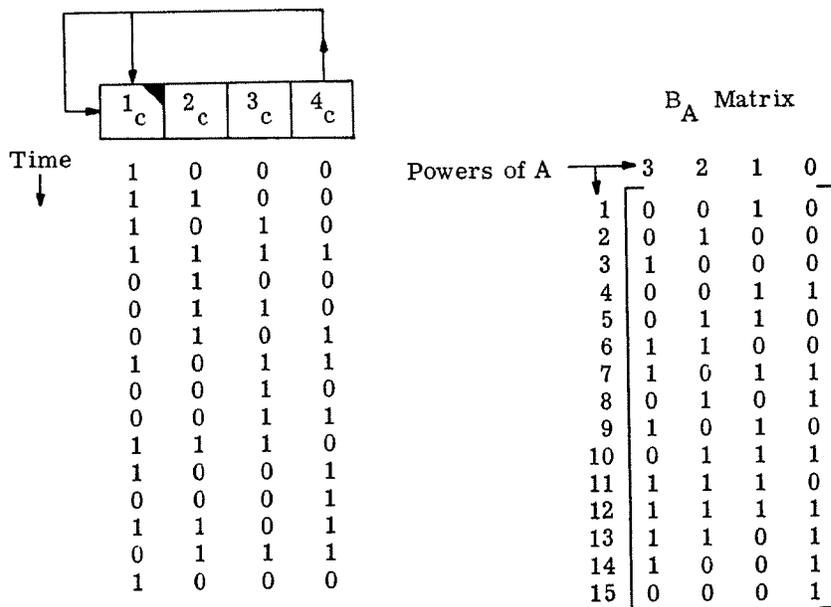| Time					Powers of A →		3	2	1	0
1	0	0	0			1	0	0	1	0
1	1	0	0			2	0	1	0	0
1	0	1	0			3	1	0	0	0
1	1	1	1			4	0	0	1	1
0	1	0	0			5	0	1	1	0
0	1	1	0			6	1	1	0	0
0	1	0	1			7	1	0	1	1
1	0	1	1			8	0	1	0	1
0	0	1	0			9	1	0	1	0
0	0	1	1			10	0	1	1	1
1	1	1	0			11	1	1	1	0
1	0	0	1			12	1	1	1	1
0	0	0	1			13	1	1	0	1
1	1	0	1			14	1	0	0	1
0	1	1	1			15	0	0	0	1
1	0	0	0							

Fig. 17. The $[4,1,0]_{MC}$ MCRG, the successive content
vectors, and the associated B_A matrix.

value determined by the shift-and-add property of maximal sequences. The shift between sequences without an interstage adder (4 in the example above) is identical to the shift between stages of the equivalent SCRG (see the example on Page 67).

Tables of the shift between sequences from adjacent stages for all maximal MCRG's of length $2 \leq n \leq 12$ are given in Section 8.4.

6.5.2 Nonmaximal MCRG with Irreducible Characteristic Polynomial. All the sequences produced by a generator with an irreducible characteristic polynomial have the same length, ℓ. A partial shift-and-add property exists. That is, for certain shifts, the shift-and-add property holds. However, for all other shifts different sequences are obtained.

The relationship between the sequences produced by adjacent stages not separated by an adder is given by Eq. 216.

$$X_i(j) = X_{i+1}(j) + X_{i+1}(j+1) \qquad (mod-2)$$

If the shift-and-add property holds for the particular characteristic polynomial for a shift of "one," then both stages of the generator will produce the same sequence but shifted in time, that is,

$$X_i(j) = X_{i+1}(j + K) \qquad (224)$$

where K is the solution to the equation

$$A^K = A + I \qquad (mod-2)$$

If the shift-and-add property does not hold for a shift of "one," then the two stages will produce different sequences.

When two adjacent stages are separated by an adder, $c_i = 1$, then the problem becomes much more complicated and will not be considered further in this report.

6.5.3 Nonmaximal MCRG with Factorable Characteristic Polynomial. If two adjacent stages are not separated by an adder, then from Eq. 216

$$X_i(j) = X_{i+1}(j) + X_{i+1}(j + 1) \qquad (mod-2)$$

and the sequence from the i-th stage will be the same as the sequence from (i+1)-th stage

90

shifted in time, if and only if, the shift-and-add property holds for the sequence $X_{i+1}(j)$ for a shift of "1." When the stages are separated by an adder, the relationship becomes more complicated.

It was pointed out in Section 2.4.2 that when the characteristic polynomial of a generator is factorable,

$$f(\xi) = f'(\xi) \; f''(\xi) \; \ldots \; f'''(\xi) \qquad (\text{mod-2})$$

the sequences associated with each of the factors are among the sequences that can be produced by that generator. Unlike the SCRG, it is possible for one stage of the MCRG to produce a maximal sequence which corresponds to one of the factors of the characteristic polynomial while other stages are producing different sequences. However, the following theorem still holds:

Theorem 11:

Given an n stage MCRG with a factorable characteristic polynomial,

$$f(\xi) = f'(\xi) \; f''(\xi) \; \ldots \; f'''(\xi) \qquad (\text{mod-2})$$

The sequences produced by each stage of the MCRG follow the same sequence law as is followed by the sequence produced by the last stage.

(Note: some stages may produce the all-zero sequence.)

Theorem 11 is proved in Appendix C.

One consequence of Theorem 11 is that if the last stage of an n stage MCRG is producing a maximal sequence associated with a particular factor, then every stage of the MCRG is producing either the same sequence or the all-zero sequence. This is demonstrated in Fig. 18 for a $[6,5,4,3,0]_{MC}$ generator with a characteristic polynomial factorable by $(6,5,4,3,0) = (2,1,0)(4,1,0)$. The sequence being produced by the last stage corresponds to the $(2,1,0)$ factor which is associated with a maximal sequence of length $L = 3$. Every other stage of the generator is also producing the $(2,1,0)$ maximal sequence except the 4th stage which is producing the all-zero sequence.

An example of an MCRG with a factorable characteristic polynomial simultaneously producing sequences which correspond to different factors is shown in Fig. 19. In Fig. 19, the $[8,6,5,4,3,2,0]_{MC}$ MCRG with a characteristic polynomial that is
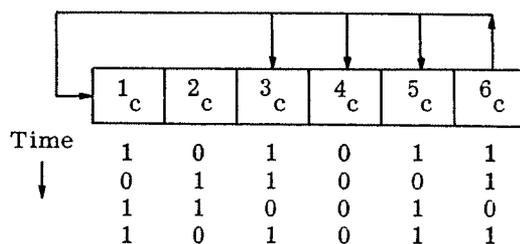
Fig. 18. A six-stage MCRG with a factorable characteristic polynomial
and one period of successive content vectors.

$(8,6,5,4,3,2,0) = (2,1,0)(3,1,0)(3,2,0) = (2,1,0)(6,5,4,3,2,1,0)$ is shown along with a

period of successive stage contents. The 4th stage is producing the maximal sequence

associated with the $(3,2,0)$ characteristic polynomial and at the same time the 5th stage is

producing the maximal sequence associated with the $(3,1,0)$ characteristic polynomial.

Theorem 11 is still satisfied, however, because the last stage is producing a $(6,5,4,3,2,1,0)$

sequence which both the $(3,1,0)$ and the $(3,2,0)$ sequences obey.
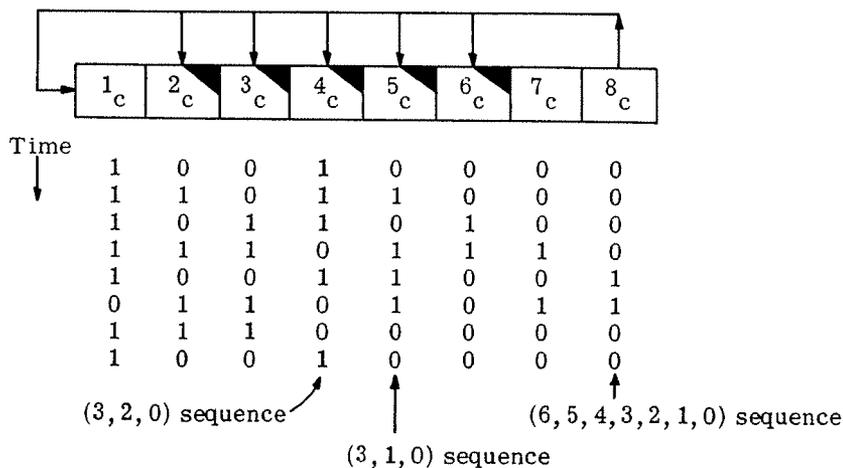
Fig. 19. The $[8,6,5,4,3,2,0]_{Mc}$ MCRG and one period of
consecutive content vectors.

6.6 The Output Adder Circuit

An output adder circuit can be used effectively with an MCRG to obtain a sequence

starting with any desired n-tuple of digits as the output of the adder when the MCRG is

initially loaded at time j with $U(j) = E_i(0)$.

Let

$$X(j) = [x(j), x(j+1), \ldots, x(j+n-1)]$$

92

represent the desired initial n-tuple of digits from the adder, and

$$\overline{\alpha} = [\alpha_1, \alpha_2, \ldots, \alpha_n]$$

be the row vector of adder taps where

α_i = 1 if the i-th adder tap is closed

= 0 otherwise

then

$$\overline{\alpha} = X(j) \cdot R_2 \qquad (\text{mod-2}) \tag{225}$$

where R_2 is defined as in Eq. 126. Expressed in series form Eq. 225 becomes

$$\alpha_i = \sum_{m=0}^{i-1} (d_m)_{i-1} \, x(j+m) \qquad (\text{mod-2}) \tag{226}$$

The derivation of Eqs. 225 and 226 is simplified by the application of the following theorem:

<u>Theorem 12</u>:

Given an n stage MCRG, if

$$u_1(j) = 1 \quad \text{and} \quad u_i(j) = 0 \quad \text{for} \quad 2 \le i \le n$$

at some time j, then

$$u_i(j+k) = (d_{i-1})_k \quad \text{for} \quad 1 \le i \le k+1, \quad 0 \le k \le n-1$$

and

$$u_i(j+k) = 0 \quad \text{for} \quad k+2 \le i \le n, \quad 0 \le k \le n-2$$

The proof of Theorem 12 is given in Appendix C.

The output of the adder in Fig. 20, given by Eq. 50, is

$$x(j+k) = \sum_{i=1}^{n} \alpha_i \, u_i(j+k) \qquad (\text{mod-2}) \tag{50}$$
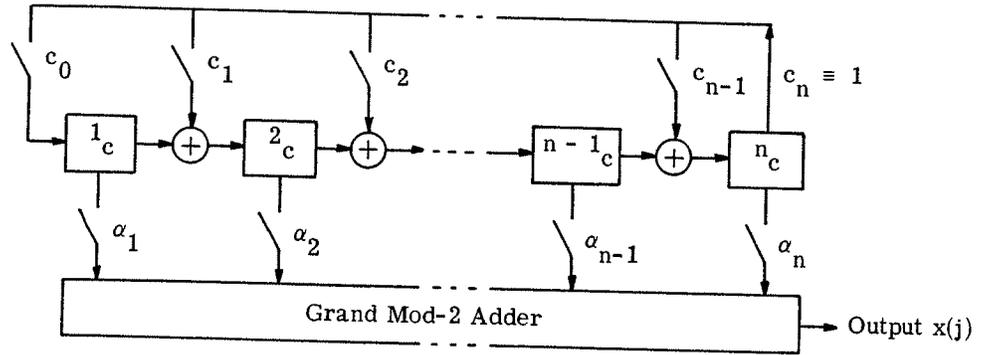
Fig. 20. An MCRG with an output adder circuit.

Applying Theorem 12, Eq. 50 becomes

$$x(j+k) = \sum_{i=1}^{k+1} (d_{i-1})_k \, \alpha_i \quad (mod\text{-}2) \qquad 0 \leq k \leq n-1 \tag{227}$$

Expressed in matrix form, Eq. 227 becomes

$$X(j) = \bar{\alpha} \, R_2 \quad (mod\text{-}2)$$

where R_2 is defined in Eq. 126 to be

$$R_2 = [r_{i,j}^2]_{n \times n}$$

$$r_{i,j}^2 = (d_{i-1})_{j-1} \quad \text{for} \quad i \leq j$$

$$= 0 \qquad \text{for} \quad i > j$$

Since R_2 is an involutory matrix, $R_2^{-1} = R_2$,

$$X(j) \cdot R_2 = \bar{\alpha} \, R_2 \cdot R_2 \quad (mod\text{-}2)$$

$$= \bar{\alpha} \, R_2 \, R_2^{-1} \quad (mod\text{-}2)$$

$$= \bar{\alpha} \tag{225}$$

which expressed in series form becomes

94

$$\alpha_i = \sum_{m=0}^{i-1} (d_m)_{i-1} \, x(j+m) \quad (\text{mod-2}) \tag{226}$$

In this section and in the one previous, we have considered complement-register generators. In particular, we have examined two canonical forms: the SCRG and the MCRG. In the next section a "hybrid" generator is considered which employs both complement stages and shift stages.

7. THE JACOBIAN HYBRID GENERATOR

In the linear sequence generators we have previously discussed, problems arise at high frequencies because of propagation times and time delays. (See Section 8.1.) One way to reduce propagation time is to build MSRG's in a circle to bring the last stage adjacent to the first and, thereby, make all feedback paths short. However, because of the operation of SRG's and CRG's all shifting and transfers must be completed before the next pulse can be introduced.

If some form of generator could be constructed which consists entirely of balanced loads and symmetric localized feedback (all paths the same and no long feedback paths), it would be useful for high frequency applications. The "Jacobian Hybrid Generator" (JHG), discussed in this section, satisfies these conditions. The JHG is composed of both shift stages and complement stages (a hybrid). It contains only localized feedback and feedforward paths. This section will present a brief treatment of the properties of the JHG.

7.1 Definition

Figure 21 shows a 7-stage JHG composed of both shift stages and complement stages. It operates as follows: the input to each stage, except the first and last stages, consists of the mod-2 sum of the output of the two adjacent stages. The input to the first stage is simply the output of the second: The input to the last stage is simply the output of the next-to-last stage. All feedback and feedforward paths are to adjacent stages so that there are no long propagation times. Each stage (except the first and last) drives two adder inputs and has a single input. In Fig. 21, stages 2, 3, 5, and 7 are complement stages, and stages 1, 4, and 6 are shift stages. The sequence obtained from any stage of the JHG is a function of those stages of the generator that are shift stages and those stages that are complement stages. It is also a function of the initial loading.

7.2 The A Matrix

Let c_i designate whether the i-th stage of a JHG is a shift stage or a complement stage, as follows

$$c_i = 1 \text{ if the i-th stage is a complement stage}$$
$$= 0 \text{ if the i-th stage is a shift stage}$$

(228)

By inspection of Fig. 21 the content of the i-th stage at time j becomes

$$u_1(j) = c_1 u_1(j-1) + u_2(j-1) \qquad \text{(mod-2)}$$

$$u_i(j) = u_{i-1}(j-1) + c_i u_i(j-1) + u_{i+1}(j-1) \qquad \text{(mod-2)} \qquad 2 \le i \le n-1$$

$$u_n(j) = u_{n-1}(j-1) + c_n u_n(j-1) \qquad \text{(mod-2)}$$

(229)

and the A matrix defined in Eq. 4 becomes

$$A = [a_{i,j}]$$

where

$$a_{i,j} = 1 \quad \text{if} \quad j = i \pm 1$$

$$a_{i,i} = c_i$$

$$a_{i,j} = 0 \quad \text{otherwise}$$

(230)

From Eq. 230 the A matrix for the JHG has the form

$$A = \begin{bmatrix} c_1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & c_2 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 1 & c_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & c_{n-2} & 1 & 0 \\ 0 & 0 & 0 & \cdots & 1 & c_{n-1} & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 & c_n \end{bmatrix}$$

(231)

Note that in Eq. 231 the A matrix for the JHG consists of all zeros except for the main diagonal and the two "off diagonals." This matrix is a "matrix of Jacobi" which is the reason for the name "Jacobian" hybrid generator.
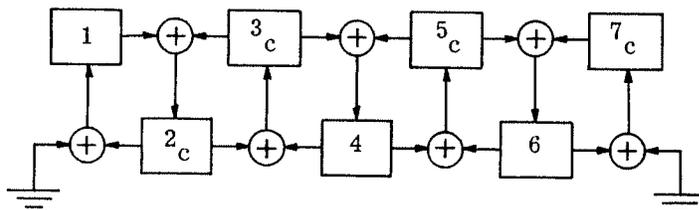
Fig. 21. A seven-stage JHG.

7.3 Characteristic Polynomial and Feedback Equation

Let $f_k(\xi)$ be the characteristic polynomial for a k-stage JHG for which $c_1, c_2, \ldots, c_k$ designate the shift and complement stages according to Eq. 228. Then by defintion $f_k(\xi)$ is the determinate

$$
f_k(\xi) = \begin{vmatrix} (c_1+\xi) & 1 & \ldots & 0 & 0 \\ 1 & (c_2+\xi) & \ldots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & (c_{k-1}+\xi) & 1 \\ 0 & 0 & \ldots & 1 & (c_k+\xi) \end{vmatrix} \quad \text{(mod-2)} \quad (232)
$$

For a 1-stage generator

$$
f_1(\xi) = \left| c_1 + \xi \right| = c_1 + \xi \quad \text{(mod-2)} \quad (233)
$$

For a 2-stage generator

$$
f_2(\xi) = \begin{vmatrix} (c_1+\xi) & 1 \\ 1 & (c_2+\xi) \end{vmatrix} = \xi^2 + (c_1+c_2)\,\xi + (c_1 c_2 + 1) \quad \text{(mod-2)} \quad (234)
$$

98

For an n-stage generator, $n \geq 3$,

$$f_n(\xi) = \begin{vmatrix} (c_1+\xi) & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & (c_2+\xi) & 1 & \cdots & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & (c_{n-2}+\xi) & 1 & 0 \\ 0 & 0 & 0 & \cdots & 1 & (c_{n-1}+\xi) & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 & (c_n+\xi) \end{vmatrix} \quad \text{(mod-2)} \quad (235)$$

Expansion of the determinate in Eq. 235 by minors along the last row gives

$$f_n(\xi) = (c_n+\xi) \begin{vmatrix} (c_1+\xi) & 1 & \cdots & 0 & 0 \\ 1 & (c_2+\xi) & \cdots & 0 & 0 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ 0 & 0 & \cdots & (c_{n-2}+\xi) & 1 \\ 0 & 0 & \cdots & 1 & (c_{n-1}+\xi) \end{vmatrix}$$

$$+ \begin{vmatrix} (c_1+\xi) & 1 & \cdots & 0 & 0 \\ 1 & (c_2+\xi) & \cdots & 0 & 0 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ 0 & 0 & \cdots & (c_{n-2}+\xi) & 0 \\ 0 & 0 & \cdots & 1 & 1 \end{vmatrix} \quad \text{(mod-2)} \quad (236)$$

Further expansion of the second determinant in Eq. 236 in the last column gives

$$f_n(\xi) = (c_n+\xi) \begin{vmatrix} (c_1+\xi) & 1 & \cdots & 0 & 0 \\ 1 & (c_2+\xi) & \cdots & 0 & 0 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ 0 & 0 & \cdots & (c_{n-2}+\xi) & 1 \\ 0 & 0 & \cdots & 1 & (c_{n-1}+\xi) \end{vmatrix}$$

$$+ \begin{vmatrix} (c_1 + \xi) & 1 & \cdots & 0 \\ 1 & (c_2 + \xi) & \cdots & 0 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & 0 & \cdots & (c_{n-2} + \xi) \end{vmatrix} \quad (\text{mod-2})$$

$$= (c_n + \xi) \, f_{n-1}(\xi) + f_{n-2}(\xi) \qquad (\text{mod-2}) \qquad (237)$$

Equations 233, 234, and 237 form a recursion relationship from which the characteristic polynomial of an n-stage JHG can be determined. Unfortunately the solution of this recursion relationship requires knowledge of all 2^{n-1} smaller characteristic polynomials to find all 2^n n-th order characteristic polynomials.

The feedback equation for a JHG is defined as follows:

$$[n; a, b, \ldots, c]_{JH} : \begin{array}{l} \underline{\text{feedback equation}} \text{ for an n-stage} \\ \text{JHG in which stages } a, b, \ldots, c \\ \text{are complement stages.} \end{array} \qquad (238)$$

For example, the feedback equation for the 7-stage JHG in Fig. 21 is $[7; 7, 5, 3, 2]_{JH}$; the feedback equation for an n-stage JHG in which every stage is a shift stage is simply $[n; \; -]_{JH}$.

Because of the symmetry of the "A" matrix of the JHG, if the A matrix is rotated 180° and the resulting matrix denoted A^R, then A^R is the "A" matrix for the same JHG if the numbering of the stages increases from right to left. However, rotating a matrix 180° does not change the characteristic polynomial, so that A and A^R have the same characteristic polynomial. This property is also evident from Fig. 21 because reversing the numbering of the stages does not change the operation of the generator. One consequence of this is that two n-stage JHG's have the same characteristic polynomial, and produce the same sequences. For example, $[3; 2, 1]_{JH}$ and $[3; 3, 2]_{JH}$, both 3-stage JHG's have the same $(3, 1, 0)$ characteristic polynomial. The feedback equation may be purely symmetric and the two feedback equations are consequently identical. For example, reversing the numbering of a $[3; 3, 2, 1]_{JH}$ gives $[3; 3, 2, 1]_{JH}$. Another consequence is that for $n \geq 2$ there will be n-th degree characteristic polynomials for which no n-stage JHG exists.

For example, this listing gives all the possible characteristic polynomials of degree $1 \leq n \leq 3$ and the feedback equations of the n-stage JHG associated with the polynomial,

Polynomial	Feedback Equation
(1)	$[1;-]_{JH}$
(1, 0)	$[1;1]_{JH}$
(2)	$[2;2,1]_{JH}$
(2, 0)	$[2;-]_{JH}$
(2, 1)	none
(2, 1, 0)	$[2;1]_{JH}$ or $[2;2]_{JH}$
(3)	$[3;-]_{JH}$
(3, 0)	none
(3, 1)	$[3;3,1]_{JH}$
(3, 2)	$[3;2]_{JH}$
(3, 1, 0)	$[3;2,1]_{JH}$ or $[3;3,2]_{JH}$
(3, 2, 0)	$[3;1]_{JH}$ or $[3;3]_{JH}$
(3, 2, 1)	none
(3, 2, 1, 0)	$[3;3,2,1]_{JH}$

From this list we can see that no JHG exists which corresponds to a (2, 1) or (3, 0) or (3, 2, 1).

Unlike the SRG's and the CRG's described in previous sections, no simple relationship or transformation between the characteristic polynomial and the feedback equation has been found for the JHG. Equations 233, 234, and 237 represent one way of determining the characteristic polynomial of an n-stage JHG. This method is well suited for compiling a table of all possible JHG's and their characteristic polynomials starting with a 1-stage generator and progressing through the n-stages. However, to find the characteristic polynomial of a particular n-stage generator for large n, when $f_{n-1}(\xi)$ and $f_{n-2}(\xi)$ are not known, a second procedure is more suitable.

This method for determining the characteristic polynomial of a JHG is based on:

<u>Theorem 13</u>:

If an n-stage JHG is initially loaded with $U(j) = E_1(0)$, that is

$$u_1(j) = 1$$

$$u_i(j) = 0 \quad \text{for} \quad 2 \leq i \leq n$$

then

$$u_k(j+k-1) = 1 \quad \text{for} \quad 1 \leq k \leq n$$

and

$$u_i(j+k-1) = 0 \quad \text{for} \quad 2 \leq k+1 \leq i \leq n$$

Theorem 13 is proved in Appendix D.

By reindexing Eq. 14, and assuming $b_n \equiv 1$, the characteristic sequence law can be written as

$$\sum_{k=0}^{n} b_k \, u_i(j+k) = 0 \quad (\text{mod-2}) \tag{239}$$

If the JHG is initially loaded with the first elementary load, $U(j) = E_1(0)$, then by Theorem 13,

$$u_i(j+k) = 0 \quad \text{for} \quad k < i-1$$

and

$$u_i(j+i-1) = 1$$

Equation 239 becomes

$$\sum_{k=i-1}^{n} b_k \, u_i(j+k) = \sum_{k=i}^{n} b_k \, u_i(j+k) + b_{i-1} = 0 \quad (\text{mod-2})$$

or

$$b_{i-1} = \sum_{k=i}^{n} b_k \, u_i(j+k) \quad (\text{mod-2}) \tag{240}$$

102

As an illustration, consider a $[5;4,3,2,1]_{JH}$ 5-stage JHG. The generator and its successive stage contents for an initial loading of $U(j) = E_1(0)$ are shown in Fig. 22. Applying Eq. 240 with $n = 5$ and $b_5 \equiv 1$

$$b_4 = b_5 \, u_5(j+5) = 0 \quad (mod-2)$$

$$b_3 = b_4 \, u_4(j+4) + b_5 \, u_4(j+5) = 0 + 0 = 0 \quad (mod-2)$$

$$b_2 = b_3 \, u_3(j+3) + b_4 \, u_3(j+4) + b_5 \, u_3(j+5) = 0 + 0 + 1 = 1 \quad (mod-2)$$

$$b_1 = b_2 \, u_2(j+2) + b_3 \, u_2(j+3) + b_4 \, u_2(j+4) + b_5 \, u_2(j+5) = 0 + 0 + 0 + 0 = 0 \quad (mod-2)$$

$$b_0 = b_1 \, u_1(j+1) + b_2 \, u_1(j+2) + b_3 \, u_1(j+3) + b_4 \, u_1(j+4) + b_5 \, u_1(j+5) \quad (mod-2)$$

$$= 0 + 0 + 0 + 0 + 1 = 1 \quad (mod-2)$$

Time					
	1	0	0	0	0
	1	1	0	0	0
	0	0	1	0	0
	0	1	1	1	0
	1	0	1	0	1
	1	0	1	0	0
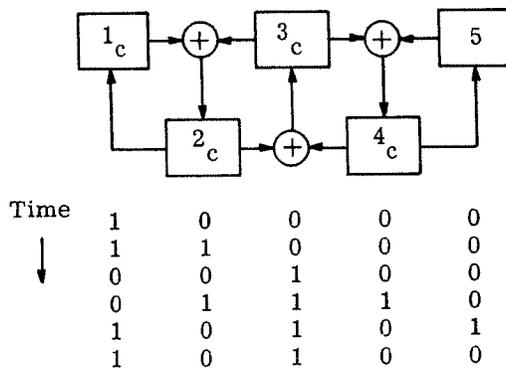
Fig. 22. The $[5,4,3,2,1]_{JH}$ and the successive content vectors.

Thus, the characteristic polynomial for the $[5;4,3,2,1]_{JH}$ 5-stage JHG is $(5,2,0)$. Since reverse feedback equations give the same characteristic polynomial, the $[5;5,4,3,2]_{JH}$ 5-stage JHG is also associated with the $(5,2,0)$ characteristic polynomial. A complete tabulation of all maximal JHG's is given in Section 8.3 for $2 \leq n \leq 12$.

As yet no practical method has been found for determining the feedback equation of a JHG associated with a given characteristic polynomial (the reverse process of above). In fact, as shown above, some characteristic polynomials do not even have an associated feedback equation.

It should be noted that if a JHG exists for every irreducible characteristic polynomial, then from Section 2.4.2 every polynomial can be obtained by employing cascaded

103

JHG's. Or it can be obtained by beating JHG's, in which the individual generators correspond to the irreducible factors of the original polynomial.

7.4 Initial Loading

Like the generators we have discussed, it is possible to find the proper initial loading for an n-stage JHG to obtain any desired n-tuple of digits from some stage of the generator.

Let $U(j)$ be the content vector of the JHG at time j, and let $V_i(j)$ be defined as in Eq. 15

$$V_i(j) = \begin{bmatrix} u_i(j) \\ u_i(j+1) \\ \cdot \\ \cdot \\ \cdot \\ u_i(j+n-1) \end{bmatrix}$$

Let $E_i(0)$ represent the i-th elementary load and be defined as the column content vector consisting of a single 1 in the i-th row, that is

$$E_i(0) = [e_j] \tag{241}$$

where

$$e_j = 1, \quad j = i$$

$$e_j = 0, \quad j \neq i \quad 1 \leq j \leq n$$

Let A be the "A" matrix for the JHG, then

$$E_i(k) = A^k E_i(0) \quad (\text{mod-2})$$

104

By inspection, this identity is true

$$
\begin{bmatrix} u_i(j) \\ u_i(j+1) \\ \cdot \\ \cdot \\ \cdot \\ u_i(j+n-1) \end{bmatrix} = \begin{bmatrix} u_1(j) & \cdots & u_i(j) & \cdots & u_n(j) \\ u_1(j+1) & \cdots & u_i(j+1) & \cdots & u_n(j+1) \\ \cdot & & \cdot & & \cdot \\ \cdot & & \cdot & & \cdot \\ \cdot & & \cdot & & \cdot \\ u_1(j+n-1) & \cdots & u_i(j+n-1) & \cdots & u_n(j+n-1) \end{bmatrix} \cdot \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \leftarrow \text{row } i \quad (\text{mod-2})
$$

$$\tag{242}$$

Equation 242 can be written

$$
V_i(j) = \begin{bmatrix} U(j)^T \\ U(j+1)^T \\ \cdot \\ \cdot \\ \cdot \\ U(j+n-1)^T \end{bmatrix} \cdot E_i(0) = \begin{bmatrix} U(j)^T \, I \\ U(j)^T \, A^T \\ \cdot \\ \cdot \\ \cdot \\ U(j)^T \, (A^{n-1})^T \end{bmatrix} \cdot E_i(0)
$$

$$
= \begin{bmatrix} U(j)^T \cdot I \cdot E_i(0) \\ U(j)^T \cdot A^T \cdot E_i(0) \\ \cdot \\ \cdot \\ \cdot \\ U(j)^T \, (A^{n-1})^T \cdot E_i(0) \end{bmatrix} \quad (\text{mod-2}) \tag{243}
$$

Since the A matrix for a JHG is symmetric about the main diagonal

$$
A^T = A
$$

and Eq. 243 becomes

$$V_i(j) = \begin{bmatrix} U(j)^T \cdot I \cdot E_i(0) \\ U(j)^T \cdot A \cdot E_i(0) \\ \cdot \\ \cdot \\ \cdot \\ U(j)^T \cdot A^{n-1} E_i(0) \end{bmatrix} \quad (\text{mod-2})$$

$$= \begin{bmatrix} U(j)^T E_i(0) \\ U(j)^T E_i(1) \\ \cdot \\ \cdot \\ \cdot \\ U(j)^T E_i(n-1) \end{bmatrix} \quad (\text{mod-2}) \qquad (244)$$

However, $U(j)^T E_i(k)$ is simply a row vector times a column vector, so

$$U(j)^T E_i(k) = E_i(k)^T U(j) \quad (\text{mod-2})$$

and Eq. 244 becomes

$$V_i(j) = \begin{bmatrix} E_i(0)^T U(j) \\ E_i(1)^T U(j) \\ \cdot \\ \cdot \\ \cdot \\ E_i(n-1)^T U(j) \end{bmatrix} \quad (\text{mod-2})$$

$$= \begin{bmatrix} E_i(0)^T \\ E_i(1)^T \\ \cdot \\ \cdot \\ \cdot \\ E_i(n-1)^T \end{bmatrix} U(j) \quad (\text{mod-2})$$

106

Assume the above n x n matrix has an inverse, P_i, that is

$$P_i = \begin{bmatrix} E_i(0)^T \\ E_i(1)^T \\ \cdot \\ \cdot \\ \cdot \\ E_i(n-1)^T \end{bmatrix}^{-1} \tag{245}$$

then

$$U(j) = P_i V_i(j) \quad (\text{mod-2}) \tag{246}$$

Applying Theorem 14, it is found that for $i = 1$, the n x n matrix

$$\begin{bmatrix} E_1(0)^T \\ \cdot \\ \cdot \\ \cdot \\ E_1(n-1)^T \end{bmatrix}$$

is a triangular matrix with all ones on the main diagonal and all zeros above, hence it is nonsingular and P_1 exists. Consequently, it is <u>always possible</u> to get any particular n-tuple of digits, $V_1(j)$, from the 1st stage of the JHG using the initial loading

$$U(j) = P_1 V_1(j) \quad (\text{mod-2}) \tag{247}$$

Unfortunately, an explicit expression for the initial loading in terms of the stage coefficients, c_i, has not been found. The important point of this section is that an initial loading <u>does exist</u> for any desired output.

7.5 Interstage Relationships

For the JHG, from Eq. 229

$$\left. \begin{aligned} u_2(j) &= c_1 u_1(j) + u_1(j+1) \quad (\text{mod-2}) \\ u_i(j) &= c_{i-1} u_{i-1}(j) + u_{i-1}(j+1) + u_{i-2}(j) \quad (\text{mod-2}) \quad 3 \le i \le n \end{aligned} \right\} \tag{248}$$

107

From the definition of sequence addition and Eq. 248 it follows that

$$X_2(j) = c_1 X_1(j) + X_1(j+1) \qquad (mod-2)$$

$$X_i(j) = c_{i-1} X_{i-1}(j) + X_{i-1}(j+1) + X_{i-2}(j) \quad (mod-2) \quad 3 < i \leq n \qquad (249)$$

where $X_i(j)$ is the sequence produced by the i-th stage of the JHG.

Define an operator τ which operates on an entire sequence $X_i(j)$ and performs the function of shifting that sequence by one digit, that is

$$\tau X_i(j) = X_i(j+1)$$

and

$$\tau^k X_i(j) = X_i(j+k) \qquad (250)$$

Then

$$X_2(j) = (c_1 + \tau) X_1(j) \qquad (mod-2) \qquad (251)$$

$$X_3(j) = (c_2 + \tau) X_2(j) + X_1(j) \qquad (mod-2)$$

$$= [(c_2 + \tau)(c_1 + \tau) + 1] X_1(j) \qquad (mod-2)$$

$$= [\tau^2 + (c_1 + c_2) \tau + (c_1 c_2 + 1)] X_1(j) \quad (mod-2) \qquad (252)$$

$$X_i(j) = (c_{i-1} + \tau) X_{i-1}(j) + X_{i-2}(j) \qquad (mod-2) \qquad (253)$$

Comparing Eqs. 251 and 252 with Eqs. 233 and 234 we see that

$$X_2(j) = f_1(\tau) X_1(j) \qquad (mod-2)$$

and

$$X_3(j) = f_2(\tau) X_1(j) \qquad (mod-2) \qquad (254)$$

where $f_k(\xi)$ is defined to be the characteristic polynomial of a k-stage JHG for which $c_1, \ldots, c_k$ designate the shift and complement stages as in Eq. 232.

Assume for some arbitrary value of k, $3 \leq k \leq n-1$ that

$$X_k(j) = f_{k-1}(\tau) X_1(j) \qquad (mod-2)$$

and

$$X_{k-1}(j) = f_{k-2}(\tau) X_1(j) \qquad (mod-2) \qquad (255)$$

108

then from Eqs. 253, 255, and 237,

$$X_{k+1}(j) = (c_k + \tau) X_k(j) + X_{k-1}(j) \qquad \text{(mod-2)}$$

$$= [(c_k + \tau) f_{k-1}(\tau) + f_{k-2}(\tau)] X_1(j) \qquad \text{(mod-2)}$$

$$= f_k(\tau) X_1(j) \qquad \text{(mod-2)} \qquad (256)$$

Equation 254 shows that Eq. 255 holds for $k = 3$, and Eq. 256 shows that if Eq. 255 is true for any arbitrary value of k such that $3 \leq k \leq n-1$, then it holds for the next larger value of k. Therefore by induction

$$X_k(j) = f_{k-1}(\tau) X_1(j) \quad \text{(mod-2)} \quad \text{for} \quad 2 \leq k \leq n \qquad (257)$$

Either Eq. 249 or Eq. 257 can be used to give the interstage relationships between the sequences produced by different stages of a JHG.

In the case of a maximal JHG, every stage will produce the same sequence, but the sequence from each stage will be shifted in time from the sequence produced by every other stage. In the case of a nonmaximal JHG, different stages may produce different sequences, and, as with the MCRG and the MSRG, it is possible under some circumstances for one or more of the stages to be producing the null sequence (all zeros) while other stages are producing nonzero sequences.

7.6 Output Adder Circuit

An output adder can be used with a JHG in the same manner that an output adder can be used with the previously discussed generators. Figure 23 shows a 6-stage $[6;5,3,2]_{JH}$ JHG with an output adder. The output of the adder is given by

$$x(j+k) = \sum_{i=1}^{n} \alpha_i u_i(j+k) \qquad \text{(mod-2)}$$

With $X(j)$ and $\bar{\alpha}$ defined as in Eqs. 51 and 52, and the content vector $U(j)$,

$$x(j+k) = \bar{\alpha} \cdot U(j+k) \qquad \text{(mod-2)}$$

$$X(j) = \bar{\alpha} [U(j), U(j+1), \ldots, U(j+n-1)] \qquad \text{(mod-2)} \qquad (258)$$

109

If the JHG is initially loaded with

$$U(j) = E_1(0)$$

then Eq. 258 becomes

$$X(j) = \bar{\alpha} \; [E_1(0), E_1(1), \dots, E_1(n-1)] \qquad (\text{mod-2})$$
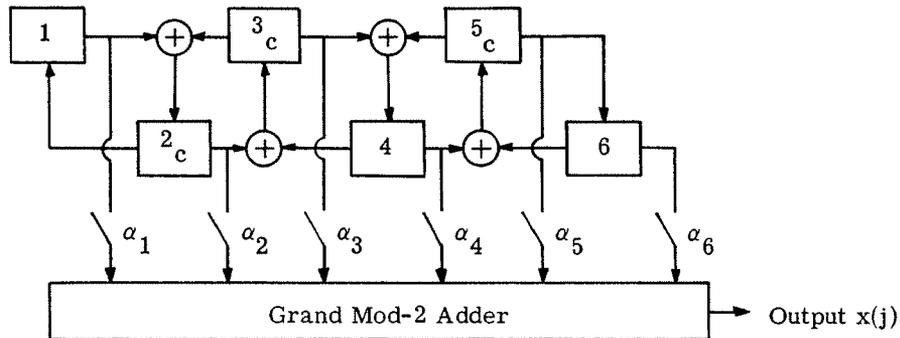
Fig. 23. A six-stage JHG with an output adder circuit.

Applying Theorem 13, the n x n matrix above is a triangular matrix with all ones on the main diagonal and all zeros below. Hence it is nonsingular and its inverse exists, therefore

$$\bar{\alpha} = X(j) \; [E_1(0), E_1(1), \dots, E_1(n-1)]^{-1} \qquad (\text{mod-2}) \qquad (259)$$

Equation 259 can be used to determine the proper adder taps to close to obtain any desired n-tuple, X(j), as the initial output of the adder when the elementary load is present. Although an explicit expression for $\bar{\alpha}$ has not been obtained, a solution has been shown to exist. Thus this technique can always be employed.

110

8. COMPARISON AND SUMMARY OF GENERATORS

In the preceding sections of this report, techniques for generating periodic linear binary sequences using the SSRG, MSRG, SCRG, MCRG, and the JHG were considered. We have shown that all of these generators (except the JHG) are equivalent; that is, for any characteristic polynomial an SSRG, MSRG, SCRG, or MCRG can be found which is associated with that polynomial. Any desired starting point of a sequence can be obtained by properly loading the generator. The output adder technique for obtaining a desired starting point applies to each type of generator. We discussed the relationship between the sequences produced by different stages of the same generator. Finally, each of the generators discussed in this report represents a "canonical" or standard form of generator.

In this section we will discuss the advantages and disadvantages of the various types of generators and summarize the mathematical relationships which described their operation. Also, two tables are presented: one showing the feedback connections for all the equivalent maximal SSRG, MSRG, SCRG, MCRG, and JHG of $2 \leq n \leq 12$ stages and another showing the shifts between the sequences produced by adjacent stages of maximal MSRG, SCRG, and MCRG of $2 \leq n \leq 12$ stages.

8.1 Advantages and Disadvantages of Different Generators

Each of the generators discussed in this report has features which makes it suitable for particular applications. Cost, high speed operation, simplicity of wiring, simplicity of the mathematics associated with the operation and availability of component parts will determine which of the generators is most practical. In the following section we will discuss some of the advantages and disadvantages of the specific types of generators we have previously reviewed.

The SSRG

Advantages

The SSRG is popular largely because of the easy mathematics which describe its operation. Hardware for it is readily available. It is

111

similar to the shift register used in digital computers. The starting conditions for "resetting" the SSRG are trivially determined. The SSRG can be easily modified for different characteristic polynomials since all feedback is external to the shift register which requires only changing the outputs of the stages. The SSRG is also useful for "digital filtering techniques" (Ref. 2) because of the simple one-bit delay between stages of the SSRG.

Disadvantages

The interstage wiring is two-wire logic consisting of either the "set-reset" type of bistable elements or the "shift-destruct" type of bistable elements. Since mod-2 adders in the feedback loop must be cascaded, long propagation and delay times may exist for the feedback signal which limits the upper frequency of operation. With multiple adder networks in the feedback loop, the shift register stages drive unbalanced loads. This imbalance can be overcome by using buffered adders; however, this increases the delay time through the adders. Because of ths shifting and feedback path return, all transfers of the register must be completed before the next shifting pulse can occur.

The MSRG

Advantages

Because the feedback adders are not cascaded, the time delay for the feedback signal is held down. The MSRG uses modular-type construction requiring two basic elements: (1) a shift stage, and (2) a shift stage and adder. The adders for the MSRG can be gate control circuits instead of conventional adders (Ref. 2). Every stage except the last has balanced loading. The MSRG is an ideal form of generator for generating sequences in a digital computer. A check of the low-order bit is required. If it is "zero," the contents of the accumulator in the computer are simply right shifted. If it is a "one," then bit-wise exclusive OR the feedback taps to the accumulator and right shift the contents. The MSRG is a common form of storage register for error correcting codes (Ref. 5). As an added feature, the MSRG can be used as a B_A matrix computer (see Section 4.6).

Disadvantages

Like the SSRG, the interstage wiring of the MSRG is two-wire logic. The starting conditions for "resetting" the MSRG are more complicated than for the SSRG. The MSRG cannot be easily modified for different characteristic polynomials because the adder network is interstage. The last stage of the generator may be required to drive many adder inputs. The return path of the generator may be physically long requiring long propagation times. Because of the shifting and feedback path return of the MSRG, all transfers of the register must be completed before the next shifting pulse can occur.

The SCRG

Advantages

The interstage connections utilize one-wire logic which is simpler than the two-wire logic used with the SRG's. In some forms, the complement stage requires fewer components to construct than the

shift stage. The feedback connections can be easily modified for different characteristic polynomials since all feedback is external to the complement register. It is possible to obtain large uniform delays between the sequences obtained from adjacent stages of the SCRG. Also, in many instances the SCRG for a given characteristic polynomial requires fewer feedback adders than does the equivalent SSRG or MSRG. As an example, for the maximal characteristic polynomial $(7, 6, 5, 4, 3, 2, 0)$ the feedback equation for the SCRG is $[7, 6, 0]_{SC}$ requiring one mod-2 adder while the equivalent SSRG and MSRG have the feedback equations $[7, 5, 4, 3, 2, 1, 0]_{SS}$ and $[7, 6, 5, 4, 3, 2, 0]_{MS}$, respectively, both requiring five mod-2 adders. On the other hand, some SCRG's require more adders than the equivalent SSRG or MSRG.

Disadvantages

The mathematics of the SCRG deals with polynomials in the variable $(1 + \xi)^k$ bringing in the mod-2 binomial coefficients which complicate the equations that describe its operation. Consequently, the starting condition for "resetting" the SCRG is more difficult than for the SSRG. Since the mod-2 adders in the feedback loop must be cascaded, long propagation time may have a feedback signal which limits the upper frequency of operation. The complement register stages drive unbalanced loads because of multiple adder networks in the feedback loop. Because of the shifting and feedback path return of the SCRG, all transfers of the register must be completed before the next shifting pulse can occur.

The MCRG

Advantages

The MCRG uses one-wire logic in its interstage connections like the SCRG. In some forms, the complement stage requires fewer components to construct than does the shift stage. The feedback adders are not cascaded, so that the time delay for the feedback signal is reduced in comparison with the time delay for the SSRG and the SCRG. Every stage except the last has balanced loading. The MCRG uses modular-type construction requiring two basic elements: (1) a complement stage, and (2) a complement stage and adder. Another feature which may be useful is the variable interstage delay between successive stages of the MCRG.

Disadvantages

The mathematics of the MCRG deals with polynomials in the variable $(1 + \xi)^k$ bringing in the mod-2 binomial coefficients which complicate the equations describing its operation. The starting conditions for "resetting" the MCRG are more complicated than those for the SSRG, MSRG, or SCRG. The feedback connections cannot easily be modified for different characteristic polynomials because the adder network is interstage. The last stage of the generator may be required to drive many adder inputs. The return path of the generator may also be physically long requiring long propagation time. Because of the shifting and feedback path return of the MCRG, all transfers of the register must be completed before the next shifting pulse can occur.

113

The JHG

Advantages

In the JHG generator, all feedback loops are localized and extend only to adjacent stages. Thus there are no long return propagation paths. Because the shifting and feedback paths are localized, the JHG is ideal for high-frequency operation. For long JHG's, the final stages can operate independently of the first stages. This feature allows the pulsing of the generator at a rate higher than the propagation time required for the pulses to propagate to the end of the generator. All of the inputs and loadings of the JHG are balanced. It is the most "modular" of all generators.

Disadvantages

We do not understand the mathematics underlying the operation of the JHG. It cannot easily be modified to a different sequence generator because the characteristic polynomial is a function of the type of stages employed. Not all of the characteristic polynomials are associated with a JHG. The minimum number of adders required is always the maximum number of adders that can be used.

8.2 Mathematical Relationships for the Different Generators (Summary)

A summary of the relationships developed for the different types of generators is given below.

1. The A Matrix: $A = [a_{i,j}]_{n \times n}$

    SSRG $\qquad a_{1,j} = c_j$

    $\qquad\qquad\quad a_{i,i-1} \equiv 1 \qquad\qquad 2 \leq i \leq n \qquad\qquad\qquad\qquad$ (34)

    $\qquad\qquad\quad a_{i,j} = 0 \qquad\qquad\quad\ \text{otherwise}$

    where c_i are the feedback taps, $c_n = c_0 \equiv 1$.

    MSRG $\qquad a_{i,n} = c_{i-1}$

    $\qquad\qquad\quad a_{i,i-1} \equiv 1 \qquad\qquad 2 \leq i \leq n \qquad\qquad\qquad\qquad$ (66)

    $\qquad\qquad\quad a_{i,j} = 0 \qquad\qquad\quad\ \text{otherwise}$

    where c_i are the feedback taps, $c_0 = c_n \equiv 1$.

114

$$\text{SCRG} \quad a_{1,1} = c_1 + 1 \qquad (\text{mod-}2)$$

$$a_{1,j} = c_j \qquad 2 \leq j \leq n$$

$$a_{j,j} = 1 \qquad 2 \leq j \leq n$$

$$a_{j,j-1} = 1 \qquad 2 \leq j \leq n$$

$$a_{i,j} = 0 \qquad \text{otherwise}$$

$$\tag{113}$$

where c_i are the feedback taps, $c_n = c_0 \equiv 1$.

$$\text{MCRG} \quad a_{j,j} = 1 \qquad 1 \leq j \leq n-1$$

$$a_{j+1,j} = 1 \qquad 1 \leq j \leq n-1$$

$$a_{i,n} = c_{i-1} \qquad 1 \leq i \leq n-1$$

$$a_{n,n} = c_{n-1} + 1 \qquad (\text{mod-}2)$$

$$a_{i,j} = 0 \qquad \text{otherwise}$$

$$\tag{188}$$

where c_i are the feedback taps, $c_0 = c_n \equiv 1$.

$$\text{JHG} \quad a_{i,i+1} = 1 \qquad 1 \leq i \leq n-1$$

$$a_{i,i} = c_i$$

$$a_{i,i-1} = 1 \qquad 2 \leq i \leq n$$

$$a_{i,j} = 0 \qquad \text{otherwise}$$

$$\tag{230}$$

where $c_i = 1$ if the i-th stage is a complement stage,

$c_i = 0$ otherwise.

2. The Characteristic Polynomial: the coefficients, b_k, of the characteristic polynomial are given in terms of the feedback taps, c_k.

$$\text{SSRG} \quad b_k = c_{n-k} \tag{38}$$

$$\text{MSRG} \quad b_k = c_k \tag{69}$$

$$\text{SCRG} \qquad b_k = \sum_{i=0}^{n-k} (d_k)_{n-i}\, c_i \qquad (\text{mod-2}) \qquad\qquad (145)$$

$$B = R_3 \cdot C \qquad (\text{mod-2}) \qquad\qquad (146)$$

$$\text{MCRG} \qquad b_k = \sum_{i=k}^{n} (d_k)_i\, c_i \qquad (\text{mod-2}) \qquad\qquad (193)$$

$$B = R_2 \cdot C \qquad (\text{mod-2}) \qquad\qquad (194)$$

JHG   no generalized equation; the characteristic polynomial may be determined by evaluating the determinant

$$f(\xi) = |A + \xi I| \qquad (\text{mod-2}) \qquad\qquad (6)$$

from the recursion relation

$$f_n(\xi) = (c_n + \xi)\, f_{n-1}(\xi) + f_{n-2}(\xi) \qquad (\text{mod-2}) \qquad\qquad (237)$$

or by the method described in Section 7.3.

3.   The Feedback Equation: the feedback taps, c_k, are determined from the coefficients, b_k, of the characteristic polynomial

$$\text{SSRG} \qquad c_k = b_{n-k} \qquad\qquad (38)$$

$$\text{MSRG} \qquad c_k = b_k \qquad\qquad (69)$$

$$\text{SCRG} \qquad c_k = \sum_{i=n-k}^{n} (d_{n-k})_i\, b_i \qquad (\text{mod-2}) \qquad\qquad (150)$$

$$C = R_3^{-1} \cdot B \qquad (\text{mod-2}) \qquad\qquad (149)$$

$$\text{MCRG} \qquad c_k = \sum_{i=k}^{n} (d_k)_i\, b_i \qquad (\text{mod-2}) \qquad\qquad (196)$$

$$C = R_2 \cdot B \qquad (\text{mod-2}) \qquad\qquad (195)$$

JHG   neither an equation nor a practical method has yet been determined for finding the feedback taps of the JHG associated with a particular characteristic polynomial.

See Section 8.3 for a table of <u>all</u> equivalent <u>maximal</u> generators of length $2 \leq n \leq 12$.

4. Initial Loading: the initial contents of the generator at time j, $\{u_1(j), u_2(j), \ldots, u_n(j)\}$, necessary to obtain a desired n-tuple of consecutive bits $\{u_n(j), u_n(j+1), \ldots, u_n(j+n-1)\}$ as the starting output of the n-th stage can be determined as follows:

SSRG $\qquad u_i(j) = u_n(j+n-i) \qquad\qquad\qquad\qquad\qquad\qquad (43)$

$\qquad\qquad\quad U(j) = I^* \cdot V_n(j) \qquad\qquad (\text{mod-2}) \qquad\qquad (45)$

MSRG $\qquad u_i(j) = \displaystyle\sum_{k=0}^{n-i} c_{i+k}\, u_n(j+k) \qquad (\text{mod-2}) \qquad\qquad (78)$

$\qquad\qquad\quad U(j) = F_M\, V_n(j) \qquad\qquad (\text{mod-2}) \qquad\qquad (80)$

SCRG $\qquad u_i(j) = \displaystyle\sum_{k=0}^{n-i} (d_k)_{n-i} \cdot u_n(j+k) \qquad (\text{mod-2}) \qquad\qquad (165)$

$\qquad\qquad\quad U(j) = R_4 \cdot V_n(j) \qquad\qquad (\text{mod-2}) \qquad\qquad (166)$

MCRG $\qquad u_i(j) = \displaystyle\sum_{m=0}^{n-i} \left[\sum_{k=i+m}^{n} (d_m)_{k-i}\, c_k \right] u_n(j+m) \qquad (\text{mod-2}) \qquad (199)$

$\qquad\qquad\quad U(j) = F_M \cdot R_1 \cdot V_n(j) \qquad\qquad (\text{mod-2}) \qquad\qquad (200)$

JHG $\qquad$ (desired output at first stage)

$\qquad\qquad\quad U(j) = P_1 \cdot V_1(j) \qquad\qquad (\text{mod-2}) \qquad\qquad (247)$

where P_1 defined by Eq. 245 is

$$
P_1 = \begin{bmatrix} E_1(0)^T \\ E_1(1)^T \\ \cdot \\ \cdot \\ \cdot \\ E_1(n-1)^T \end{bmatrix}^{-1}
$$

5. Interstage Relationships: depending upon the type of generator used and upon whether it is maximal, two different stages, i and k, may produce (1) the same sequence, $X_i(j) = X_k(j)$; (2) the same sequence but shifted in time, $X_i(j) = X_k(j+J_{i,k})$; (3) entirely different sequences. Regardless of the relationship, every sequence produced by a generator will obey the sequence law of the generator. A summary of these relationships for the generators discussed in this report is given below.

SSRG: For every SSRG,

$$X_i(j) = X_{i+k}(j+k) \tag{48}$$

MSRG: (1) The maximal MSRG,

If two adjacent stages, i and i+1, are not separated by an interstage adder, then

$$X_i(j) = X_{i+1}(j+1) \tag{82}$$

If the two stages are separated by an interstage adder, then

$$X_i(j) = X_{i+1}(j+J_{i,i+1}) \tag{83}$$

The shift $J_{i,i+1}$ between the i-th stage and the (i+1)-th stage can be determined from the B_A matrix for the generator using the procedure described in Section 4.5.1.

(2) The nonmaximal MSRG,

If two adjacent stages, i and i+1, are not separated by an interstage adder, then as in the maximal case

$$X_i(j) = X_{i+1}(j+1)$$

If the two stages are separated by an interstage adder, then they may produce the same sequences

shifted in time or they may produce different sequences depending on the partial shift-and-add property of the nonmaximal sequence.

SCRG: For every SCRG,

$$V_{i-1}(j) = H \cdot V_i(j) \quad (\text{mod-2}) \quad 2 \leq i \leq n \tag{167}$$

and if $c_n = 1$, then

$$V_i(j) = G \cdot V_{i-1}(j) \quad (\text{mod-2}) \quad 2 \leq i \leq n \tag{171}$$

(1) Maximal SCRG:

$$X_{i-1}(j) = X_i(j+K) \tag{174}$$

where K can be found from the B_A matrix as the solution to the equation $A^K = A + I \quad (\text{mod-2})$ \hfill (175)

(2) Nonmaximal SCRG with irreducible characteristic polynomial, if the shift-and-add property holds for a shift of 1, then every stage produces the same sequence shifted in time; otherwise, if there are m different sequences that obey the characteristic sequence law of the generator, then every set of k <u>consecutive</u> stages of the SCRG (k $\leq$ m) will produce k different sequences.

(3) Nonmaximal SCRG with factorable characteristic polynomial, if $c_n = 1$ and $\sum_{i=0}^{n} c_i = 1$, then the sequences produced by every stage of the SCRG will obey the same sequence law (Theorem 8).

MCRG: (1) Maximal MCRG,

If two adjacent stages are not separated by an interstage adder,

$$X_i(j) = X_{i+1}(j+K) \tag{217}$$

where K can be determined from the B_A matrix

as the solution to the equation

$$A^K = A + I \qquad (\text{mod-2})$$

If two adjacent stages are separated by an inter-

stage adder, then

$$X_i(j) = X_{i+1}(j + J_{i,i+1})$$

and $J_{i,i+1}$ can be determined by the method

discussed in Section 6.5.1.

(2) Nonmaximal MCRG with irreducible characteristic

    polynomial, for two stages, i and i+1, not separated

    by an interstage adder, if the shift-and-add property

    holds for a shift of 1 then

$$X_i(j) = X_{i+1}(j+K) \qquad\qquad\qquad (224)$$

    where K is the solution to the equation

$$A^K = A + I \qquad (\text{mod-2})$$

    otherwise, the two sequences will be different.

(3) Maximal MCRG with factorable characteristic

    polynomial, the sequence produced by each

    stage of the MCRG obeys the same sequence

    law as the sequence produced by the last stage

    (Theorem 11).

See Section 8.4 for a table of interstage shifts for all maximal generators,

except the JHG, of length $2 \leq n \leq 12$.

6. Output Adder Circuit: the adder taps, α_i, which must be closed to obtain a

specific n-tuple $[x(j), x(j+1), \ldots, x(j+n-1)]$, as the initial output of the adder

when the generator is initially loaded with $U(j) = E_1(0)$ can be determined

from the following equations.

SSRG: $\quad \alpha_i = \displaystyle\sum_{k=1}^{i} c_{i-k}\, x(j+k-1) \qquad \text{(mod-2)} \qquad$ (62)

$\quad \bar{\alpha} = X(j) \cdot F_A \qquad \text{(mod-2)} \qquad$ (61)

MSRG: $\quad \alpha_i = x(j+i-1) \qquad\qquad$ (108)

$\quad \bar{\alpha} = X(j) \qquad\qquad$ (109)

SCRG: $\quad \alpha_i = \displaystyle\sum_{m=1}^{i} \left[\sum_{k=0}^{i-m} (d_{m-1})_{i-1-k}\, c_k \right] x(j+m-1) \qquad \text{(mod-2)} \qquad$ (180)

$\quad \bar{\alpha} = X(j) \cdot R_2 \cdot F_A \qquad \text{(mod-2)} \qquad$ (179)

MCRG: $\quad \alpha_i = \displaystyle\sum_{m=0}^{i-1} (d_m)_{i-1}\, x(j+m) \qquad \text{(mod-2)} \qquad$ (226)

$\quad \bar{\alpha} = X(j) \cdot R_2 \qquad \text{(mod-2)} \qquad$ (225)

JHG: $\quad \bar{\alpha} = X(j) \cdot [E_1(0), E_1(1), \ldots, E_1(n-1)]^{-1} \qquad \text{(mod-2)} \qquad$ (259)

$\quad = X(j)\, P_1^{T} \qquad \text{(mod-2)}$

8.3 Equivalent Maximal Generators

Table I shows all the maximal characteristic polynomials of degree $2 \leq n \leq 12$ and their associated SSRG, MSRG, SCRG, MCRG, and JHG's. The polynomials and feedback equations are given in octal form to conserve space. An example is given below to illustrate the use of the table.

Example

Consider the $(7,5,4,3,0)$ maximal characteristic polynomial. To find the octal representation of this polynomial, write the coefficients in descending order as a sequence of ones and zeros, i.e.,

$$\text{exponent} \rightarrow 7\ 6\ 5\ 4\ 3\ 2\ 1\ 0$$

$$\text{polynomial} \rightarrow 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1$$

Group the binary representation by threes, adding zeros on the left if necessary. The above polynomial then becomes

$$0 \ 1 \ 0, \ 1 \ 1 \ 1, \ 0 \ 0 \ 1$$

This is a binary number which can be converted to an octal number using the following conversions:

Binary	=	Octal
0 0 0	=	0
0 0 1	=	1
0 1 0	=	2
0 1 1	=	3
1 0 0	=	4
1 0 1	=	5
1 1 0	=	6
1 1 1	=	7

Under this transformation

$$0 \ 1 \ 0 \rightarrow 2$$
$$1 \ 1 \ 1 \rightarrow 7$$
$$0 \ 0 \ 1 \rightarrow 1$$

and the octal representation of the polynomial is 271.

Looking in Table I under $N = 7$ (for a 7-stage register), the characteristic polynomial, 271, is found in the first column labeled POLY. Reading across the row, the octal representations of the feedback equations associated with this polynomial are given.

POLY	SSRG	MSRG	SCRG	MCRG	JHG	
271	235	271	313	323	211	310

The feedback equations for the SSRG, MSRG, SCRG, and MCRG are found by expanding the octal numbers. That is,

For the SSRG,

$$\text{feedback taps} \rightarrow \quad 7 \ 6, \ 5 \ 4 \ 3, \ 2 \ 1 \ 0$$

$$235 = 0 \ 1 \ 0, \ 0 \ 1 \ 1, \ 1 \ 0 \ 1 \rightarrow [7,4,3,2,0]_{SS}$$

Table I

EQUIVALENT GENERATORS FOR N = 8

POLY	SSRG	MSRG	SCRG	MCRG	JHG	
00435	00561	00435	00661	00433	00406	00540
00453	00651	00453	00771	00477	00537	00772
00455	00551	00455	00471	00471	00466	00756
00515	00545	00515	00765	00537	00623	00554
00537	00765	00537	00545	00545	00513	00711
00543	00615	00543	00515	00543	00455	00722
00545	00515	00545	00615	00567	00471	00664
00561	00455	00561	00735	00551	00417	00634
00607	00435	00607	00537	00455	00471	00760
00615	00543	00615	00477	00477	00757	00524
00651	00453	00651	00607	00771	00452	00567
00703	00607	00703	00453	00703	00505	00642
00717	00747	00717	00613	00651	00535	00672
00747	00717	00747	00763	00643	00547	00732
00765	00537	00765	00543	00637	00713	00723
				00615	00653	00725

EQUIVALENT GENERATORS FOR N = 9

POLY	SSRG	MSRG	SCRG	MCRG	JHG	
01021	01041	01021	01443	01423	01162	01234
01033	01541	01033	01743	01437	01056	01350
01041	01021	01041	01063	01461	01431	01461
01055	01321	01055	01563	01473	01415	01541
01063	01461	01063	01423	01443	01152	01254
01131	01151	01131	01113	01511	01243	01612
01137	01751	01137	01713	01517	01341	01514
01151	01131	01151	01533	01553	01047	01416
01157	01731	01157	01333	01555	01035	01710
01167	01371	01167	01473	01563	01377	01776
01175	01605	01175	01773	01577	01276	01560
01207	01425	01207	01137	01751	01006	01372
01225	01243	01225	01317	01715	01633	01300
01243	01425	01243	01517	01713	01475	01663
01257	01725	01257	01617	01707	01044	01571
01275	01665	01267	01157	01731	01547	01110
01317	01365	01275	01257	01725	01517	01715
01321	01715	01317	01167	01671	01327	01745
01333	01055	01321	01267	01641	01201	01726
01365	01555	01333	01207	01665	01365	01402
01371	01275	01365	01707	01617	01173	01536
01423	01175	01371	01021	01605	01137	01674
01425	01243	01423	01041	01021	01433	01615
01437	01743	01425	01641	01027	01523	01691
01443	01423	01437	01461	01033	01427	01721
01461	01063	01443	01021	01063	01316	01625
01517	01713	01461	01321	01041	01236	01346
01533	01563	01517	01751	01055	01263	01362
01541	01033	01533	01511	01137	01057	01632
01555	01553	01541	01231	01113	01315	01546
01563	01333	01553	01131	01145	01361	01750
01577	01473	01555	01731	01151	01067	01436
01605	01773	01563	01371	01157	01001	01730
01667	01207	01577	01175	01175	01217	01742
01707	01267	01605	01555	01371	01013	01604
01713	01617	01665	01275	01275	01103	01412
01715	01317	01671	01055	01555	01241	01576
01725	01257	01707	01725	01321	01375	01733
01731	01437	01725	01425	01245	01667	01302
01743	01137	01731	01365	01243	01206	01144
01751	01577	01751	01145	01275	01114	01260
01773	—	01773	01245	01267	01032	01230
			01605	01231	01062	01340
				01225	01016	01771
				01207	01477	01501
					01405	

EQUIVALENT GENERATORS FOR N = 2

POLY	SSRG	MSRG	SCRG	MCRG	JHG	
00007	00007	00007	00007	00007	00005	00006
00007	00007	00007	00007	00007	00005	00006

EQUIVALENT GENERATORS FOR N = 3

POLY	SSRG	MSRG	SCRG	MCRG	JHG	
00013	00015	00013	00013	00015	00013	00016
00015	00013	00015	00015	00013	00011	00014

EQUIVALENT GENERATORS FOR N = 4

POLY	SSRG	MSRG	SCRG	MCRG	JHG	
00023	00031	00023	00031	00023	00025	00032
00031	00023	00031	00037	00037	00033	00035

EQUIVALENT GENERATORS FOR N = 5

POLY	SSRG	MSRG	SCRG	MCRG	JHG	
00045	00051	00045	00073	00067	00057	00076
00051	00045	00051	00057	00075	00046	00054
00057	00075	00057	00067	00073	00043	00070
00067	00073	00067	00051	00045	00041	00060
00073	00067	00073	00075	00057	00047	00074
00075	00057	00075	00045	00051	00063	00071

EQUIVALENT GENERATORS FOR N = 6

POLY	SSRG	MSRG	SCRG	MCRG	JHG	
00103	00141	00103	00165	00127	00106	00130
00133	00155	00133	00111	00111	00135	00156
00141	00103	00141	00163	00147	00126	00132
00147	00163	00147	00103	00141	00145	00151
00155	00133	00155	00133	00155	00125	00152
00163	00147	00163	00127	00165	00101	00140

EQUIVALENT GENERATORS FOR N = 7

POLY	SSRG	MSRG	SCRG	MCRG	JHG	
00203	00301	00203	00277	00375	00315	00331
00211	00221	00211	00217	00361	00256	00272
00217	00361	00217	00357	00367	00307	00361
00221	00211	00221	00367	00357	00227	00364
00235	00271	00235	00247	00343	00253	00352
00247	00345	00247	00323	00313	00222	00244
00253	00325	00253	00203	00301	00357	00373
00277	00235	00277	00313	00323	00211	00310
00301	00255	00301	00253	00253	00241	00302
00313	00375	00313	00345	00247	00204	00220
00323	00203	00323	00235	00277	00333	00355
00325	00323	00325	00375	00235	00267	00366
00345	00313	00345	00271	00221	00275	00336
00357	00253	00357	00211	00217	00225	00334
00361	00247	00361	00221	00211	00213	00350
00367	00217	00367	00361	00203	00305	00324
00375	00357	00375	00301	—	00216	00321
	00277				00246	00270
						00262

123

Table I (Cont.)

N = 11 (Cont.)

POLY	SSRG	MSRG	SCRG	MCRG	JMG

EQUIVALENT GENERATORS FOR N = 10

POLY	SSRG	MSRG	SCRG	MCRG	JMG

EQUIVALENT GENERATORS FOR N = 11

POLY	SSRG	MSRG	SCRG	MCRG	JMG

Table I (Cont.)

N = 12 (Cont.)

POLY	SSRG	MSRG	SCRG	MCRG	JMG

N = 11 (Cont.)

POLY	SSRG	MSRG	SCRG	MCRG	JMG

EQUIVALENT GENERATORS FOR N = 12

POLY	SSRG	MSRG	SCRG	MCRG	JMG

Table I (Cont.)

N = 12 (Cont.)

POLY	SSRG	MSRG	SCRG	MCRG		JHG
16021	10407	16021	15033	15413	11413	16414
16027	16407	16027	13033	15415	11773	16774
16047	16207	16047	17233	15457	12505	15052
16115	13107	16115	12133	15505	12445	15112
16207	16047	16207	14373	15743	11611	14434
16237	17447	16237	13773	15775	10135	15640
16245	12247	16245	14573	15723	11245	15124
16273	15647	16273	15173	15713	10331	14660
16305	12147	16305	12673	15665	10631	14630
16311	11147	16311	17673	15677	10561	14350
16317	17147	16317	11673	15671	13103	16046
16363	14747	16363	10473	15621	10155	15540
16407	16027	16407	13413	15035	13753	16576
16443	14227	16443	15213	15053	10255	15520
16503	14127	16503	13113	15115	10515	15450
16521	10527	16521	17513	15137	11261	14324
16533	15527	16533	14513	15123	11521	14254
16565	12727	16565	11313	15151	11305	15064
16605	12067	16605	10353	15341	10703	16070
16611	11067	16611	15353	15353	10343	16160
17025	12417	17025	13003	14015	13376	13766
17031	11417	17031	16003	14007	17267	17327
17057	17217	17057	14203	14043	12216	13422
17105	12117	17105	11103	14111	12776	13772
17121	10517	17121	13503	14135	10554	11550
17147	16317	17147	11703	14171	14451	14511
17163	14717	17163	13303	14155	16013	16403
17217	17057	17217	17343	14357	10076	13700
17343	14357	17343	14043	14203	11072	12704
17421	10437	17421	11023	14411	14423	16211
17433	15437	17433	12023	14405	10526	13250
17447	16237	17447	13223	14455	11416	13414
17561	10737	17561	17323	14557	11132	12644
17631	11477	17631	11763	14771	12262	12322
17673	15677	17673	11163	14711	14065	15301
17675	13677	17675	17163	14717	12226	13222
17711	11177	17711	13663	14675	16007	17003

For the MSRG,

$$\text{feedback taps} \rightarrow \quad 7\ 6, \quad 5\ 4\ 3, \quad 2\ 1\ 0$$

$$271 = 0\ 1\ 0, \quad 1\ 1\ 1, \quad 0\ 0\ 1 \rightarrow [7,5,4,3,0]_{MS}$$

For the SCRG,

$$\text{feedback taps} \rightarrow \quad 7\ 6, \quad 5\ 4\ 3, \quad 2\ 1\ 0$$

$$313 = 0\ 1\ 1, \quad 0\ 0\ 1, \quad 0\ 1\ 1 \rightarrow [7,6,3,1,0]_{SC}$$

For the MCRG,

$$\text{feedback taps} \rightarrow \quad 7\ 6, \quad 5\ 4\ 3, \quad 2\ 1\ 0$$

$$323 = 0\ 1\ 1, \quad 0\ 1\ 0, \quad 0\ 1\ 1 \rightarrow [7,6,4,1,0]_{MC}$$

To find the feedback equations for the JHG, remember that there is no zero term in the feedback equation. The conversion from the octal representation proceeds as follows: from the table, the two JHG equations which are associated with the 271 characteristic polynomial are represented by the octal numbers 211 and 310. Begin numbering the feedback taps starting on the far right with 1 instead of 0 and neglect the leading 1 on the left.[10] The transformation of octal number 211 then becomes

$$\text{feedback taps} \rightarrow \quad 7, \quad 6\ 5\ 4, \quad 3\ 2\ 1$$

$$211 = 0\ \underline{1}\ 0, \quad 0\ 0\ 1, \quad 0\ 0\ 1 \rightarrow [7;4,1]_{JH}$$
$$\uparrow$$
$$- \text{ neglect}$$

and

$$\text{feedback taps} \rightarrow \quad 7, \quad 6\ 5\ 4, \quad 3\ 2\ 1$$

$$310 = 0\ \underline{1}\ 1, \quad 0\ 0\ 1, \quad 0\ 0\ 0 \rightarrow [7;7,4]_{JH}$$
$$\uparrow$$
$$- \text{ neglect}$$

---

[10]The leading 1 in the octal representation of the feedback law for the JHG permits defining the length n of the generator and also makes each octal feedback equation unique. This leading 1 represents the "n"; in the feedback equation of the JHG.

It should be noticed that the two equivalent JHG's, the $[7;4,1]_{JH}$ and the $[7;7,4]_{JH}$ are simply reverses of each other as explained in Section 7.3.

The reverse polynomial of the POLY entry in Table I is the same as the SSRG octal feedback equation if it is considered as a characteristic polynomial. Note that the MSRG feedback law is identical to the characteristic polynomial, however, it has been included in Table I for completeness.

The maximal JHG entries in Table I were determined by considering every possible 2^n feedback equations and finding the corresponding characteristic polynomial using Eqs. 233, 234, and 237. A list of all maximal characteristic polynomials was compiled and a search procedure was used to select those feedback equations which correspond to maximal characteristic polynomials. Note that every maximal characteristic polynomial has two corresponding JHG's and the tendency is to conclude that every maximal polynomial has a JHG; however, this statement has not been proved.

8.4 Interstage Shift for Maximal Generators

Table II gives the time shifts between the sequences produced by adjacent stages for all maximal MSRG, SCRG, and MCRG of length $2 \leq n \leq 12$. For an SSRG the shift is always 1 between stages and is not shown in the table. The following example illustrates the use of Table II.

Example

Consider the $(5,3,2,1,0)$ maximal characteristic polynomial. The octal representation of this polynomial is 57. From Table II under N = 5, one finds

POLY	SCRG	MSRG	MCRG
57	12	1, 20, 17, 23	12, 11, 26, 1

For the SCRG the shift between adjacent stages is always the same and from Table II this shift is found to be K = 12. Thus

$$X_i(j) = X_{i+1}(j+12) \qquad 1 \leq i \leq n-1$$

The feedback law for the MSRG (from Table I) is $[5,3,2,1,0]_{MS}$ and there are interstage adders between Stages 1 and 2, 2 and 3, and 3 and 4. The first entry under "MSRG" in Table II is 1. This "1" indicates that there is a shift of 1 between stages that

128

Table II

SHIFT BETWEEN SEQUENCES FROM ADJACENT STAGES WHICH ARE SEPARATED BY AN ADDER FOR GENERATORS OF LENGTH N=2

POLY	SCRG	MSRG	MCRG
00007	2	1,2,	2,1,
00007	2	1,2,	2,1,

SHIFT BETWEEN SEQUENCES FROM ADJACENT STAGES WHICH ARE SEPARATED BY AN ADDER FOR GENERATORS OF LENGTH N=3

POLY	SCRG	MSRG	MCRG
00013	3	1,5,	3,1,
00015	5	1,5,	5,4,

SHIFT BETWEEN SEQUENCES FROM ADJACENT STAGES WHICH ARE SEPARATED BY AN ADDER FOR GENERATORS OF LENGTH N=4

POLY	SCRG	MSRG	MCRG
00023	4	1,12,	4,3,
00031	12	1,12,	12,11,6,1,

SHIFT BETWEEN SEQUENCES FROM ADJACENT STAGES WHICH ARE SEPARATED BY AN ADDER FOR GENERATORS OF LENGTH N=5

POLY	SCRG	MSRG	MCRG
00045	18	1,27,	18,17,8,1,
00051	14	1,27,	14,12,21,1,
00057	12	1,20,17,23,	12,11,26,1,
00067	19	1,13,28,19,	19,17,
00073	13	1,19,28,13,	13,12,4,20,
00075	20	1,23,17,20,	20,13,

SHIFT BETWEEN SEQUENCES FROM ADJACENT STAGES WHICH ARE SEPARATED BY AN ADDER FOR GENERATORS OF LENGTH N=6

POLY	SCRG	MSRG	MCRG
00103	6	1,58,	6,5,44,59,
00133	56	1,8,44,48,	56,35,
00141	58	1,58,	58,57,20,1,
00147	25	1,39,59,25,	25,1,
00155	8	1,48,4,8,	8,6,32,1,
00163	39	1,25,59,39,	39,37,34,1,

SHIFT BETWEEN SEQUENCES FROM ADJACENT STAGES WHICH ARE SEPARATED BY AN ADDER FOR GENERATORS OF LENGTH N=7

POLY	SCRG	MSRG	MCRG
00203	7	1,121,	7,5,105,74,55,1,
00211	31	1,121,	31,27,102,1,
00217	87	1,41,118,91,	87,86,118,33,96,1,
00221	97	1,121,	97,96,72,120,25,1,
00235	118	1,19,68,36,	118,116,46,1,
00247	114	1,14,49,100,	114,113,65,1,
00253	21	1,107,102,41,	21,1,
00271	10	1,36,68,19,	10,9,77,1,
00277	19	1,109,26,65,15,37,	19,17,33,1,
00301	121	1,121,	121,120,23,84,
00313	39	1,89,122,35,	39,38,97,90,
00323	89	1,39,122,85,	89,29,83,40,
00325	107	1,41,102,107,	107,106,115,97,81,22,
00345	14	1,100,49,14,	14,12,63,123,
00357	55	1,73,23,122,105,55,	55,51,
00361	41	1,91,118,41,	41,8,
00367	73	1,55,105,123,23,73,	73,72,105,39,
00375	109	1,17,165,26,109,	109,108,

SHIFT BETWEEN SEQUENCES FROM ADJACENT STAGES WHICH ARE SEPARATED BY AN ADDER FOR GENERATORS OF LENGTH N=8

POLY	SCRG	MSRG	MCRG
00435	25	1,206,202,57,	25,24,177,184,
00453	243	1,3,172,65,	243,242,165,64,226,104,
00455	240	1,31,183,36,	240,186,60,84,
00515	23	1,210,250,45,	23,22,196,103,141,234,
00537	122	1,134,197,71,117,243,	122,120,155,135,
00543	197	1,59,53,138,	197,195,35,60,
00545	233	1,45,25,210,	233,232,109,924,
00551	16	1,36,183,31,	16,66,123,241,
00561	231	1,97,202,206,	231,230,173,135,18,26,
00607	99	1,157,244,69,	99,247,218,152,105,1,
00615	59	1,138,53,59,	59,57,18,109,148,1,
00651	13	1,65,172,13,	13,12,177,1,
00703	157	1,99,244,157,	157,5,229,1,
00717	141	1,115,235,250,21,141,	141,140,174,1,
00747	115	1,141,21,25,235,115,	115,114,21,207,77,1,
00765	134	1,243,117,71,197,134,	134,132,217,1,

SHIFT BETWEEN SEQUENCES FROM ADJACENT STAGES WHICH ARE SEPARATED BY AN ADDER FOR GENERATORS OF LENGTH N=9

POLY	SCRG	MSRG	MCRG
01021	130	1,503,	130,129,112,1,
01033	197	1,315,218,83,	197,196,72,320,156,1,
01041	382	1,503,	382,378,395,150,326,1,
01055	275	1,473,468,75,	275,274,193,150,326,1,
01063	104	1,408,195,413,	104,103,294,1,
01131	140	1,176,506,540,	140,448,244,11,
01137	53	1,340,506,170,	53,52,382,223,42,1,
01151	372	1,419,436,102,12,269,	372,371,244,398,53,1,
01157	93	1,419,436,102,12,269,	93,91,481,46,31,1,
01167	443	1,69,163,324,241,211,	443,442,501,381,480,210,1,
01175	234	1,44,63,235,27,134,	234,233,333,133,185,481,210,1,
01207	194	1,318,311,287,	194,193,161,342,446,119,394,1,
01225	226	1,60,505,461,	226,251,375,29,484,1,
01243	36	1,470,469,71,	36,34,330,243,270,1,
01245	786	1,451,504,60,	286,285,101,486,274,1,
01257	453	1,59,280,31,447,394,	453,452,288,348,165,1,
01267	461	1,51,280,333,447,410,	461,286,422,340,173,1,
01275	26	1,460,442,470,106,51,	26,24,380,179,334,1,
01317	441	1,71,263,350,435,370,	441,241,178,1,
01321	237	1,75,460,471,	237,440,396,464,306,1,
01333	501	1,11,341,506,181,490,	501,499,129,247,186,1,
01355	486	1,51,106,470,442,460,	486,485,309,150,177,1,
01371	278	1,134,2,229,63,444,	278,276,99,1,
01423	114	1,398,504,1114,	114,110,
01427	476	1,71,465,476,	476,475,235,11,
01437	428	1,84,136,12,338,426,	428,427,302,280,
01443	398	1,114,504,598,	398,397,449,343,
01461	208	1,43,195,78,	408,313,
01473	249	1,263,23,47,436,269,	249,247,24,279,
01517	135	1,377,470,84,263,135,	135,134,470,309,172,419,
01533	126	1,386,18,8,160,126,	126,125,351,301,
01541	315	1,403,218,215,	315,313,83,269,
01553	386	1,126,16,728,18,386,	386,424,114,212,
01555	11	1,490,181,7,56,341,1,	11,10,197,33,132,305,
01563	263	1,249,436,47,23,263,	263,262,456,461,19,305,
01577	404	1,108,139,77,134,144,14,404,	404,402,413,488,177,481,
01605	318	1,387,311,218,	318,199,410,374,105,195,
01617	327	1,185,376,15,25,136,327,	327,325,425,390,432,186,
01665	51	1,410,447,33,288,951,	51,50,117,256,33,462,
01671	69	1,211,241,734,163,69,	69,65,99,444,
01707	185	1,327,136,5,25,376,185,	185,184,136,232,424,328,
01713	377	1,135,263,284,470,377,	377,375,293,136,
01715	71	1,370,434,290,263,71,	71,70,84,442,
01725	59	1,394,447,341,288,59,	59,57,17,136,122,454,
01731	419	1,260,12,40,436,419,	419,418,76,24,267,94,
01743	84	1,428,338,12,156,84,	84,35,246,429,
01751	459	1,234,429,25,382,459,	459,457,312,54,
01773	108	1,404,14,14,134,77,139,108,	108,107,373,405,

Table II (Cont.)

N = 11 (Cont.)

SHIFT BETWEEN SEQUENCES FROM
ADJACENT STAGES WHICH ARE SEPARATED
BY AN ADDER FOR GENERATORS OF LENGTH N=10

POLY	SCRG	MSRG	MCRG

SHIFT BETWEEN SEQUENCES FROM
ADJACENT STAGES WHICH ARE SEPARATED
BY AN ADDER FOR GENERATORS OF LENGTH N=11

POLY	SCRG	MSRG	MCRG

Table II (Cont.)

N = 11 (Cont.)

POLY	SCRG	MSRG	MCRG

(Dense multi-column numerical table of polynomial and shift-register generator data for N = 11. Individual entries not legibly resolvable.)

SHIFT BETWEEN SEQUENCES FROM
ADJACENT STAGES WHICH ARE SEPARATED
BY AN ADDER FOR GENERATORS OF LENGTH N=12

POLY	SCRG	MSRG	MCRG

N = 12 (Cont.)

POLY	SCRG	MSRG	MCRG

(Dense multi-column numerical table of polynomial and shift-register generator data for N = 12. Individual entries not legibly resolvable.)

131

Table II (Cont.)

N = 12 (Cont.)

POLY	SCRG	MSRG	MCRG
15723	3709	1,387,4031,3360,3487,2124,3372,3709,	3709,3707,3303,2094,1787,1,
16005	2368	1,3455,2358,2368,	2368,2367,1738,2996,3269,2325,34,1,
16021	1808	1,959,1319,1808,	1808,1807,596,677,693,1,
16027	1401	1,2695,2202,4086,1893,1401,	1401,1399,3279,1077,817,1,
16047	3498	1,598,2615,4086,1481,3498,	3498,3497,2615,284,3296,2893,2684,1,
16115	3678	1,835,1453,3038,3274,3678,	3678,3676,62,1578,1697,1,
16207	598	1,3498,1481,4086,2615,598,	598,597,1305,2556,2220,3039,3672,1,
16237	1266	1,2830,2269,3391,2637,2155,1827,1266,	1266,1264,2555,1355,3920,167,1492,287,1541,1
16245	244	1,3608,3312,3156,1958,244,	244,243,764,840,3163,2286,3768,1,
16273	2250	1,1846,1919,2891,2619,1873,2977,2250,	2250,2249,3744,422,3926,802,2176,1,
16305	3857	1,477,513,2938,3493,3857,	3857,3855,1444,3069,1612,3751,3838,1,
16311	3014	1,2466,2065,937,3792,3014,	3014,3013,304,1627,1799,2904,2087,189,3604,1
16317	55	1,4041,1428,2559,3662,1962,2668,55,	55,1426,1161,332,2326,1386,1283,1,
16363	1564	1,2532,1626,310,7,988,1158,1564,	1564,1560,2712,3147,2107,1,
16407	2695	1,1401,1892,4086,2203,2695,	2695,2693,502,3010,3594,1,
16443	2696	1,1400,2961,867,259,2696,	2696,2695,1821,2751,2525,1,
16503	3304	1,792,3422,3468,1292,3304,	3304,3302,2640,2233,1456,1,
16521	3692	1,1613,126,1754,998,3692,	3692,3691,3098,189,836,3330,3155,1,
16533	2935	1,1161,4051,883,271,1496,1483,2935,	2935,2934,1297,3844,44,1,
16565	2771	1,2649,2511,3405,7,2192,2840,2771,	2771,1254,2735,3017,2261,1,
16605	2642	1,2907,1226,3616,1887,2642,	2642,1868,687,659,2861,1,
16611	4032	1,2597,1987,2037,1625,4032,	4032,4031,3205,552,3654,1527,3725,1,
17025	2475	1,3241,1616,3708,1242,2475,	2475,2473,3916,1,
17031	582	1,1206,1136,3533,1726,582,	582,581,2370,1,
17057	2219	1,1877,365,99,4087,3997,441,2219,	2219,2218,2380,1,
17105	1509	1,1078,2576,1975,1043,1509,	1509,3051,3842,1,
17121	761	1,1052,753,1941,3676,761,	761,759,2142,2330,1726,1,
17147	4041	1,55,2668,1962,3662,2559,1428,4041,	4041,2666,2935,2904,62,1,
17163	620	1,3476,563,1054,1232,2919,2416,620,	620,618,3732,2661,933,1,
17217	1877	1,2219,441,3997,4087,99,3655,1877,	1877,1876,441,3311,4040,2793,2723,1,
17343	1358	1,2738,2674,1869,925,3283,3528,1358,	1358,1357,2800,1,
17421	2367	1,2818,2359,3276,1458,2367,	2367,2636,630,1,
17433	774	1,3322,2382,480,3773,1862,3781,774,	774,772,451,1,
17447	2830	1,1266,1827,2155,2637,3391,2269,2830,	2830,2828,1452,3203,1371,1,
17561	3096	1,3997,27,1668,1395,2338,3854,3096,	3096,3095,242,1853,829,2675,395,1,
17631	843	1,2854,3690,1130,2077,2130,3651,843,	843,443,732,2618,1863,3589,2919,1,
17673	1217	1,2879,3281,3591,1108,2721,3241,3548,2981,1217	1217,1113,987,1303,362,1,
17675	86	1,3924,104,2536,3320,2947,3288,3197,1070,86	86,85,3026,1239,3577,554,3373,1,
17711	3022	1,3683,2602,1141,3977,3485,2559,3022,	3022,3020,4064,534,3786,3342,2903,1,

*

6

are not separated by an interstage adder. The second number is 20, this indicates that there is a jump of 20 across the _first_ _interstage_ _adder_ which is between Stages 1 and 2. The third number, 17, indicates a jump of 17 across the second interstage adder which is between Stages 2 and 3, the fourth number, 23, indicates a jump of 23 across the third interstage adder which is between Stages 3 and 4. Thus for the $[5,3,2,1,0]_{MS}$ MSRG

$$X_1(j) = X_2(j+20)$$

$$X_2(j) = X_3(j+17)$$

$$X_3(j) = X_4(j+23)$$

$$X_4(j) = X_5(j+1)$$

(Note: the first entry under MSRG is always 1 even though every stage of the MSRG is separated by an adder. For example for the $[2,1,0]_{MS}$ MSRG, the leading entry should be ignored.)

For the MCRG the feedback law (from Table I) is $[5,4,3,1,0]_{MC}$ and there are interstage adders between Stages 1 and 2, 3 and 4, and 4 and 5. The first entry under MCRG is 12, indicating a jump of 12 between stages not separated by an interstage adder. The next three numbers, 11, 26, and 1, indicate jumps of 11, 26, and 1 across the first, second and third interstage adders which in this case occur between Stages 1 and 2, 3 and 4, and 4 and 5, respectively. Thus for the $[5,4,3,1,0]_{MC}$ MCRG

$$X_1(j) = X_2(j+11)$$

$$X_2(j) = X_3(j+12)$$

$$X_3(j) = X_4(j+26)$$

$$X_4(j) = X_5(j+1)$$

(Note: the first entry under MCRG always indicates the jumps between stages not separated by an adder even though every stage in the generator is separated by an adder, as with the $[4,3,2,1,0]_{MC}$ MCRG. In this case the leading entry should be ignored.)

For the MCRG the shift between stages not separated by an adder is the same as the shift between stages of the SCRG having the same characteristic polynomial. This is

133

analogous to the shift of 1 between stages not separated by an adder in the MSRG and the shift of 1 between stages in the SSRG.

The following theorems which deal with the general properties of linear binary sequence generators, were presented without proof in Section 2.

Theorem 2:

Every stage of a maximal sequence generator produces the same sequence, but the sequence (except for the null sequence) from any stage will be shifted in time from the sequence produced by any other stage.

Proof

Since, by definition, a maximal sequence from an n-stage generator contains every nonzero, n-tuple of binary digits, and since any n-tuple of digits from a sequence and the characteristic sequence law completely determine the sequence, there is one and only one nonzero sequence which obeys the sequence law of a maximal generator. By Eq. 14 in the text, the sequences produced by every stage of a generator obey the same sequence law. Therefore, every stage of a maximal generator must be producing the same sequence (or the all-zero sequence).

Finally, suppose two different stages, i and k, are producing the same nonzero sequences with no time shift. There occur at most $2^n - 2$ different content vectors and hence the period is at most $2^n - 2$. But this contradicts our assumption that we were producing maximal sequences.

Theorem 4:

Let the characteristic polynomial $f(\xi)$ have the form

$$f(\xi) = \xi^k \sum_{i=k}^{n} b_i \, \xi^{i-k} \quad (\text{mod-2})$$

where

$$b_n = b_k = 1$$

135

then:

a) The sequence obtained from any stage of the generator may begin
with a transient of k or fewer bits (not part of the periodic sequence)
after which the sequence becomes periodic and obeys the sequence
law of an n - k stage generator with characteristic polynomial

$$f'(\xi) = \sum_{i=k}^{n} b_i \xi^{i-k} \quad (\text{mod-2})$$

(Note: the sequence may start out with up to k transient bits and then
produce the null sequence.)

b) There is at least one nonzero content vector, U', so that if the gener-
ator is initially loaded with U', there will be one transient content
vector before every stage produces the null sequence.

c) If the generator is capable of producing any nonzero periodic sequence
(k < n), then there is at least one nonzero content vector, U", so that
if the generator is initially loaded with U" there will be exactly one
transient content vector before the generator output becomes periodic
and at least one stage produces a nonzero sequence.

Proof

a) Let A be the "A" matrix for a generator whose characteristic polynomial is

$$f(\xi) = \xi^k (b_n \xi^{n-k} + b_{n-1} \xi^{n-k-1} + \ldots + b_{k+1} \xi + b_k) \quad (\text{mod-2}) \qquad (A-1)$$

where

$$b_k = b_n = 1$$

Let U(j+m), $m \geq 0$, be the content vector of this generator which is initially loaded with U(j).
From Eq. 3

$$A^r U(j) = U(j+r) \quad (\text{mod-2})$$

136

and by Eqs. 11 and A-1

$$f(A) = A^n + b_{n-1} A^{n-1} + \ldots + b_{k+1} A^{k+1} + b_k A^k = 0 \qquad (\text{mod-2})$$

and for $m \geq 0$

$$f(A) U(j+m) = U(j+m+n) + b_{n-1} U(j+m+n-1) + \ldots + b_{k+1} U(j+m+k+1)$$

$$+ b_k U(j+m+k) = 0 \qquad (\text{mod-2})$$

or for $m \geq 0$

$$U(j+m+n) = b_{n-1} U(j+m+n-1) + \ldots + b_{k+1} U(j+m+k+1) + b_k U(j+m+k) \qquad (\text{mod-2})$$

from which follows

$$u_i(j+m+n) = b_{n-1} u_i(j+m+n-1) + \ldots + b_{k+1} u_i(j+m+k+1) + b_k u_i(j+m+k) \qquad (\text{mod-2})$$

$$(A-2)$$

Let $V_i'(j+m)$ represent an $(n-k)$-tuple of successive output bits from the i-th stage of the generator

$$V_i'(j+m) = \begin{bmatrix} u_i(j+m+k) \\ u_i(j+m+k+1) \\ . \\ . \\ . \\ u_i(j+m+n-1) \end{bmatrix}_{(n-k) \times 1} \qquad m \geq 0 \qquad (A-3)$$

and let C_f' be the companion matrix corresponding to the polynomial

$$f'(\xi) = b_n \xi^{n-k} + b_{n-1} \xi^{n-k-1} + \ldots + b_{k+1} \xi + b_k \qquad (\text{mod-2}) \qquad (A-4)$$

$$C_f' = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ b_k & b_{k+1} & b_{k+2} & & b_{n-2} & b_{n-1} \end{bmatrix}_{(n-k) \times (n-k)} \qquad (A-5)$$

137

Then by Eq. A-2, (see Section 2.2 of text), with $m = 0$

$$C_f' \, V_i'(j) = V_i'(j+1) \quad \text{(mod-2)} \qquad \text{(A-6)}$$

and by successive application of Eq. A-6

$$(C_f')^m \, V_i'(j) = V_i'(j+m) \quad \text{(mod-2)}$$

Expanding C_f' by minors along the 1st column, remembering that $b_k = 1$, it is seen that

$$|C_f'| = b_k = 1 \quad \text{(mod-2)}$$

hence $(C_f')^{-1}$ exists and

$$V_i'(j) = (C_f')^{-m} \, V_i'(j+m) \quad \text{(mod-2)} \qquad \text{(A-7)}$$

From Eq. A-7 it is seen that $V_i'(j)$ can be uniquely determined from $V_i'(j+m)$ for any $m \geq 0$; consequently, there can be no transient bits in $V_i'(j)$. But $V_i'(j)$ is made up of bits $u_i(j+k), \ldots, u_i(j+n)$, so that the only possible transient bits are the k bits $u_i(j)$, $u_i(j+1), \ldots,$ $u_i(j+k-1)$. Note from Eq. A-2 that after the first n bits have been produced, the remaining portions of the sequence obey the characteristic sequence law,

$$u_i(j+p) = \sum_{i=1}^{n-k} b_{n-i} \, u_i(j+p-i) \quad \text{(mod-2)} \qquad p \geq n$$

which is the sequence law for an n-k stage generator whose characteristic polynomial is

$$f'(\xi) = b_n \, \xi^{n-k} + b_{n-1} \, \xi^{n-k-1} + \ldots + b_{k+1} \, \xi + b_k \quad \text{(mod-2)}$$

b) If ξ^k is a factor of $f(\xi)$, then the determinant of the A matrix for the generator with characteristic polynomial $f(\xi)$ is (Ref. 3)

$$|A| = b_0 = 0 \quad \text{(mod-2)}$$

and there is at least one vector, U', such that

$$A U' = 0 \quad \text{(mod-2)}$$

(U' can be any nonzero vector in the kernel of the linear transformation represented by the

matrix A; Ref. 3.) If the generator is initially loaded with $U(j) = U'$, then for $r \geq 1$

$$U(j+r) = A^r \cdot U(j) = A^{r-1} \cdot A \cdot U' = A^{r-1} \cdot 0 = 0 \quad \text{(mod-2)}$$

and every stage of the generator is seen to produce the null sequence.

c) Assume the generator is capable of producing a nonzero periodic sequence after all transient bits have passed. Let $U(j+s)$ be one of the nonzero periodic content vectors. Let $U'' = U(j+s) + U'$ where U' is a nonzero vector defined as in Part b) of this theorem.

Then

$$A U'' = A U(j+s) + A U' = A U(j+s) = U(j+s+1) \quad \text{(mod-2)}$$

which is the content vector which normally follows $U(j+s)$ in periodic sequence. Since $U(j+s+1)$ is preceded by $U(j+s)$ in the periodic sequence, and $U'' \neq U(j+s)$, then U'' is not a part of the periodic sequence of content vectors and is therefore by definition a transient.

APPENDIX B

The following theorems and derivations were presented without proof or full justification in Section 5. They deal with the simple complement-register generators.

I* and R_i Matrices

Define $\underline{I^*}$ as

where

$$I^* = I_{\text{rotated } 90^\circ} = \left[i^*_{j,k} \right]_{n \times n}$$

$$i^*_{j,k} = \delta_{j,n+1-k} = 1 \quad \text{when} \quad j = n+1-k$$

$$= 0 \quad \text{otherwise}$$

$$\left. \begin{array}{l} \\ \\ \\ \\ \end{array} \right\} \quad \text{(B-1)}$$

Any matrix Q such that $Q^2 = I$ is called <u>involutory</u>; an involutory matrix is its own inverse. It will now be shown that I^* is involutory:

Let

$$(I^*)^2 = \left[q_{j,k} \right]_{n \times n} \quad \text{(mod-2)}$$

where

$$q_{j,k} = \sum_{m=1}^{n} i^*_{j,m} \, i^*_{m,k} \quad \text{(mod-2)}$$

$$= \sum_{m=1}^{n} \delta_{j,n+1-m} \, \delta_{m,n+1-k} \quad \text{(mod-2)}$$

$$= \delta_{j,k} = 1 \quad \text{when} \quad j = k$$

$$= 0 \quad \text{otherwise}$$

Thus

$$(I^*)^2 = I \quad \text{(mod-2)} \quad \text{(B-2)}$$

140

and

$$(I^*)^{-1} = I^* \tag{B-3}$$

$$(I^*)^T = [p_{k,j}]_{n \times n}$$

where

$$p_{k,j} = i^*_{j,k}$$

$$= \delta_{j,n+1-k}$$

$$= \delta_{k,n+1-j}$$

$$= i^*_{k,j}$$

so

$$(I^*)^T = I^* \tag{B-4}$$

Define R_1 as

$$R_1 = [r^1_{i,j}]_{n \times n}$$

where

$$\left. \begin{array}{l} R_1 = [r^1_{i,j}]_{n \times n} \\[2ex] r^1_{i,j} = (d_{j-1})_{i-1} \quad \text{for} \quad j \leq i \\[2ex] \qquad = \quad 0 \qquad \text{for} \quad j > i \end{array} \right\} \tag{B-5}$$

That is, R_1 has the form

$$R_1 = \begin{bmatrix} (d_0)_0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ (d_0)_1 & (d_1)_1 & 0 & \cdots & 0 & 0 & 0 \\ (d_0)_2 & (d_1)_2 & (d_2)_2 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ (d_0)_{n-3} & (d_1)_{n-3} & (d_2)_{n-3} & \cdots & (d_{n-3})_{n-3} & 0 & 0 \\ (d_0)_{n-2} & (d_1)_{n-2} & (d_2)_{n-2} & \cdots & (d_{n-3})_{n-2} & (d_{n-2})_{n-2} & 0 \\ (d_0)_{n-1} & (d_1)_{n-1} & (d_2)_{n-1} & \cdots & (d_{n-3})_{n-1} & (d_{n-2})_{n-1} & (d_{n-1})_{n-1} \end{bmatrix}_{n \times n} \tag{B-6}$$

It will now be shown that $R_1^2 = I$, and hence, $R_1^{-1} = R_1$.

Let

$$R_1 \cdot R_1 = [c_{i,j}]_{n \times n} \qquad (\text{mod-2})$$

then

$$c_{i,j} = \sum_{k=1}^{n} r_{i,k}^1 \cdot r_{k,j}^1 \qquad (\text{mod-2})$$

Now

$$r_{i,k}^1 = 0 \quad \text{for} \quad i < k$$

and

$$r_{k,j}^1 = 0 \quad \text{for} \quad k < j$$

Therefore, for $i < j$

$$c_{i,j} = \sum_{k=1}^{i} r_{i,k}^1 \cdot 0 + \sum_{k=i+1}^{j-1} 0 \cdot 0 + \sum_{k=j}^{n} 0 \cdot r_{k,j}^1 \qquad (\text{mod-2})$$

$$= 0 \qquad \qquad (\text{B-7})$$

For $i \geq j$

$$c_{i,j} = \sum_{k=1}^{j-1} r_{i,k}^1 \cdot 0 + \sum_{k=j}^{i} r_{i,k}^1 \cdot r_{k,j}^1 + \sum_{k=i+1}^{n} 0 \cdot r_{k,j}^1 \qquad (\text{mod-2})$$

$$= \sum_{k=j}^{i} (d_{k-1})_{i-1} \, (d_{j-1})_{k-1} \qquad (\text{mod-2})$$

When $i = j$ this becomes

$$c_{i,i} = (d_{i-1})_{i-1} \, (d_{i-1})_{i-1} \qquad (\text{mod-2})$$

$$= 1 \cdot 1$$

$$= 1 \qquad \qquad (\text{B-8})$$

For $i > j$, let $i = j + m$ where $m = 1, 2, \ldots, n-j$, then

$$c_{i,j} = c_{j+m,j} = \sum_{k=j}^{j+m} (d_{k-1})_{j+m-1} (d_{j-1})_{k-1} \quad (\text{mod-2})$$

and by reindexing

$$c_{j+m,j} = \sum_{k=0}^{m} (d_{j-1+k})_{j-1+m} (d_{j-1})_{j-1+k} \quad (\text{mod-2}) \tag{B-9}$$

From Ref. 4, p. 61, for positive integers n, k

$$\sum_{\nu=0}^{k} (-1)^{\nu} \binom{n}{\nu} \binom{n-\nu}{k-\nu} = 0 \tag{B-10}$$

Considering Eq. B-10 in mod-2 arithmetic the term $(-1)^{\nu}$ becomes simply 1 and

$$\sum_{\nu=0}^{k} \binom{n}{\nu} \binom{n-\nu}{k-\nu} = 0 \quad (\text{mod-2}) \tag{B-11}$$

Reversing the order of summation in Eq. B-11

$$\sum_{\nu=0}^{k} \binom{n}{k-\nu} \binom{n-k+\nu}{\nu} = 0 \quad (\text{mod-2}) \tag{B-12}$$

Using the relationship $\binom{n}{i} = \binom{n}{n-i}$ Eq. B-12 becomes

$$\sum_{\nu=0}^{k} \binom{n}{n-k+\nu} \binom{n-k+\nu}{n-k} = 0 \quad (\text{mod-2}) \tag{B-13}$$

Let $j = n-k+1$ so that $k = n-j+1$ and $j \leq n$, Eq. B-13 becomes

$$\sum_{\nu=0}^{n-j+1} \binom{n}{j-1+\nu} \binom{j-1+\nu}{j-1} = 0 \quad (\text{mod-2})$$

and letting $m = n-j+1$ so that $n = j-1+m$ and $m \geq 1$

$$\sum_{\nu=0}^{m} \binom{j-1+m}{j-1+\nu} \binom{j-1+\nu}{j-1} = 0 \quad (\text{mod-2}) \tag{B-14}$$

Since mod-2 arithmetic is being used Eq. B-14 can be written for $m \geq 1$

$$\sum_{\nu=0}^{m} (d_{j-1+\nu})_{j-1+m} (d_{j-1})_{j-1+\nu} = 0 \quad (\text{mod-2}) \tag{B-15}$$

Comparing Eqs. B-15 and B-9 it is seen that for $m \geq 1$

$$c_{j+m,j} = 0$$

or

$$c_{i,j} = 0 \quad \text{for} \quad i > j \qquad \text{(B-16)}$$

Summarizing Eqs. B-7, B-8, and B-16

$$c_{i,j} = 1 \quad \text{when} \quad i = j$$

$$= 0 \quad \text{otherwise}$$

Hence

$$R_1^2 = I \qquad (\text{mod-2})$$

and

$$R_1^{-1} = R_1 \qquad \text{(B-17)}$$

Define R_2 as
$$R_2 = R_1^T = [r^2{}_{i,j}]_{n \times n}$$

where

$$r^2{}_{i,j} = (d_{i-1})_{j-1} \quad \text{for} \quad i \leq j$$

$$= 0 \qquad \text{for} \quad i > j$$

$$\left. \right\} \qquad \text{(B-18)}$$

From Eq. B-18 it is seen that R_2 has the form

$$R_2 = \begin{bmatrix}
(d_0)_0 & (d_0)_1 & (d_0)_2 & \cdots & (d_0)_{n-3} & (d_0)_{n-2} & (d_0)_{n-1} \\
0 & (d_1)_1 & (d_1)_2 & \cdots & (d_1)_{n-3} & (d_1)_{n-2} & (d_1)_{n-1} \\
0 & 0 & (d_2)_2 & \cdots & (d_2)_{n-3} & (d_2)_{n-2} & (d_2)_{n-1} \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & (d_{n-3})_{n-3} & (d_{n-3})_{n-2} & (d_{n-3})_{n-1} \\
0 & 0 & 0 & \cdots & 0 & (d_{n-2})_{n-2} & (d_{n-2})_{n-1} \\
0 & 0 & 0 & \cdots & 0 & 0 & (d_{n-1})_{n-1}
\end{bmatrix}_{n \times n} \qquad \text{(B-19)}$$

144

The inverse of R_2, R_2^{-1} becomes

$$R_2^{-1} = (R_1^T)^{-1} = (R_1^{-1})^T = (R_1)^T = R_2 \qquad \text{(B-20)}$$

Define R_3 as

$$R_3 = [r^3_{i,j}]_{n \times n}$$

where

$$r^3_{i,j} = (d_{i-1})_{n-j} \quad \text{for} \quad i \le n+1-j$$

$$= 0 \quad \text{for} \quad i > n+1-j$$

$$\left. \right\} \qquad \text{(B-21)}$$

$$R_3 = \begin{bmatrix} (d_0)_{n-1} & (d_0)_{n-2} & (d_0)_{n-3} & \cdots & (d_0)_2 & (d_0)_1 & (d_0)_0 \\ (d_1)_{n-1} & (d_1)_{n-2} & (d_1)_{n-3} & \cdots & (d_1)_2 & (d_1)_1 & 0 \\ (d_2)_{n-1} & (d_2)_{n-2} & (d_2)_{n-3} & \cdots & (d_2)_2 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ (d_{n-3})_{n-1} & (d_{n-3})_{n-2} & (d_{n-3})_{n-3} & \cdots & 0 & 0 & 0 \\ (d_{n-2})_{n-1} & (d_{n-2})_{n-2} & 0 & \cdots & 0 & 0 & 0 \\ (d_{n-1})_{n-1} & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}_{n \times n} \qquad \text{(B-22)}$$

Consider the product $R_2 \cdot I^*$

$$R_2 \cdot I^* = [q_{k,j}]_{n \times n} = [r^2_{k,j}]_{n \times n} \cdot [i^*_{k,j}]_{n \times n} \qquad \text{(mod-2)}$$

$$q_{k,j} = \sum_{m=1}^{n} r^2_{k,m} \cdot i^*_{m,j} \qquad \text{(mod-2)}$$

$$= \sum_{m=k}^{n} (d_{k-1})_{m-1} \cdot \delta_{m,n+1-j} \qquad \text{(mod-2)}$$

$$= \begin{cases} (d_{k-1})_{n-j} & \text{for} \quad k \le n+1-j \\ \\ 0 & \text{for} \quad k > n+1-j \end{cases}$$

$$= r^3_{k,j}$$

145

so

$$R_3 = R_2 \cdot I^* \quad (\text{mod-2}) \qquad \text{(B-23)}$$

$$R_3^{-1} = (R_2 \cdot I^*)^{-1} = (I^*)^{-1} \cdot R_2^{-1} = I^* \cdot R_2 \quad (\text{mod-2})$$

$$= [i^*_{j,k}]_{n \times n} \cdot [r^2_{j,k}]_{n \times n} = [p_{j,k}]_{n \times n} \quad (\text{mod-2}) \qquad \text{(B-24)}$$

where

$$p_{j,k} = \sum_{m=1}^{n} i^*_{j,m} \cdot r^2_{m,k} \quad (\text{mod-2})$$

$$= \sum_{m=1}^{k} \delta_{j,n+1-m} \cdot (d_{m-1})_{k-1} \quad (\text{mod-2})$$

$$= \begin{cases} (d_{n-j})_{k-1} & \text{for} \quad k \geq n+1-j \\[2ex] 0 & \text{for} \quad k < n+1-j \end{cases} \qquad \text{(B-25)}$$

From Eq. B-25 R_3^{-1} has the form

$$R_3^{-1} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & (d_{n-1})_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & (d_{n-2})_{n-2} & (d_{n-2})_{n-1} \\ 0 & 0 & 0 & \cdots & (d_{n-3})_{n-3} & (d_{n-3})_{n-2} & (d_{n-3})_{n-1} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & (d_2)_2 & \cdots & (d_2)_{n-3} & (d_2)_{n-2} & (d_2)_{n-1} \\ 0 & (d_1)_1 & (d_1)_2 & \cdots & (d_1)_{n-3} & (d_1)_{n-2} & (d_1)_{n-1} \\ (d_0)_0 & (d_0)_1 & (d_0)_2 & \cdots & (d_0)_{n-3} & (d_0)_{n-2} & (d_0)_{n-1} \end{bmatrix}_{n \times n} \qquad \text{(B-26)}$$

Comparing Eqs. B-22 and B-26 it is seen that

$$R_3^{-1} = R_3 \text{ rotated } 180^{\circ} \qquad \text{(B-27)}$$

146

Define R_4 as

$$R_4 = R_3^T = [r^4_{i,j}]$$

where

$$r^4_{i,j} = (d_{j-1})_{n-i} \quad \text{for} \quad j \leq n+1-i$$

$$= \quad 0 \quad \text{for} \quad j > n+1-i$$

(B-28)

$$R_4 = \begin{bmatrix} (d_0)_{n-1} & (d_1)_{n-1} & (d_2)_{n-1} & \cdots & (d_{n-3})_{n-1} & (d_{n-2})_{n-1} & (d_{n-1})_{n-1} \\ (d_0)_{n-2} & (d_1)_{n-2} & (d_2)_{n-2} & \cdots & (d_{n-3})_{n-2} & (d_{n-2})_{n-2} & 0 \\ (d_0)_{n-3} & (d_1)_{n-3} & (d_2)_{n-3} & \cdots & (d_{n-3})_{n-3} & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ (d_0)_2 & (d_1)_2 & (d_2)_2 & \cdots & 0 & 0 & 0 \\ (d_0)_1 & (d_1)_1 & 0 & \cdots & 0 & 0 & 0 \\ (d_0)_0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}_{n \times n}$$

(B-29)

The inverse of R_4, R_4^{-1} becomes

$$R_4^{-1} = (R_3^T)^{-1} = (R_3^{-1})^T = [p_{j,k}]^T = [s_{j,k}]$$

(B-30)

where

$$s_{j,k} = p_{k,j}$$

Using Eq. B-25

$$s_{j,k} = (d_{n-k})_{j-1} \quad \text{for} \quad j \geq n+1-k$$

$$= \quad 0 \quad \text{for} \quad j < n+1-k$$

(B-31)

147

and R_4^{-1} has the form

$$R_4^{-1} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & (d_0)_0 \\ 0 & 0 & 0 & \cdots & 0 & (d_1)_1 & (d_0)_1 \\ 0 & 0 & 0 & \cdots & (d_2)_2 & (d_1)_2 & (d_0)_2 \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ 0 & 0 & (d_{n-3})_{n-3} & \cdots & (d_2)_{n-3} & (d_1)_{n-3} & (d_0)_{n-3} \\ 0 & (d_{n-2})_{n-2} & (d_{n-3})_{n-2} & \cdots & (d_2)_{n-2} & (d_1)_{n-2} & (d_0)_{n-2} \\ (d_{n-1})_{n-1} & (d_{n-2})_{n-1} & (d_{n-3})_{n-1} & \cdots & (d_2)_{n-1} & (d_1)_{n-1} & (d_0)_{n-1} \end{bmatrix}_{n \times n} \tag{B-32}$$

Comparing Eqs. B-29 and B-32 it is seen that

$$R_4^{-1} = R_4 \text{ rotated } 180^{\text{o}} \tag{B-33}$$

From Eqs. B-23 and B-18

$$R_3 = R_2 \, I^* = R_1^T \cdot I^* \quad \text{(mod-2)} \tag{B-34}$$

From Eq. B-28

$$R_3^T = R_4$$

so

$$R_4^T = (R_3^T)^T = R_3 \tag{B-35}$$

Combining Eqs. B-34 and B-35

$$R_3 = R_1^T \, I^* = R_2 \, I^* = R_4^T \quad \text{(mod-2)} \tag{B-36}$$

From Eqs. B-36 and B-4

$$R_4 = (R_4^T)^T = (R_1^T \, I^*)^T = (I^*)^T \, (R_1^T)^T = I^* \, R_1 \quad \text{(mod-2)}$$

$$= (R_2 \, I^*)^T = (I^*)^T \, R_2^T = I^* \, R_2^T \quad \text{(mod-2)}$$

$$= R_3^T$$

or

$$R_4 = I^* R_1 = I^* R_2^T = R_3^T \quad (\text{mod-2}) \tag{B-37}$$

From Eqs. B-2 and B-37

$$R_1 = I^* \cdot I^* \cdot R_1 = I^* R_4 \quad (\text{mod-2})$$

$$= I^* R_3^T \quad (\text{mod-2}) \tag{B-38}$$

and from Eqs. B-18 and B-38

$$R_1 = R_2^T$$

so

$$R_1 = R_2^T = I^* R_3^T = I^* R_4 \quad (\text{mod-2}) \tag{B-39}$$

From Eqs. B-39 and B-4

$$R_2 = (R_2^T)^T = R_1^T$$

$$= (I^* R_3^T)^T = (R_3^T)^T (I^*)^T = R_3 I^* \quad (\text{mod-2})$$

$$= (I^* R_4)^T = R_4^T (I^*)^T = R_4^T I^* \quad (\text{mod-2})$$

or

$$R_2 = R_1^T = R_3 I^* = R_4^T I^* \quad (\text{mod-2}) \tag{B-40}$$

G and H Matrices

Consider an n-stage SCRG with feedback taps, c_i, and characteristic polynomial $f(\xi) = \sum_{i=0}^{n} b_i \xi^i$. From Eq. 16

$$C_f V_i(j) = V_i(j+1) \quad (\text{mod-2})$$

where C_f is the companion matrix associated with the characteristic polynomial $f(\xi)$. From Eq. 159, for an SCRG

$$u_{i-1}(j) = u_i(j) + u_i(j+1) \quad (\text{mod-2})$$

149

which leads to the equation

$$V_{i-1}(j) = V_i(j) + V_i(j+1) \qquad (\text{mod-}2)$$

$$= (C_f + I) V_i(j) \qquad (\text{mod-}2) \tag{B-41}$$

If a matrix H is defined as

$$H \equiv C_f + I \qquad (\text{mod-}2) \tag{B-42}$$

then

$$H = [h_{i,j}]_{n \times n}$$

where

$$h_{i,j} = \delta_{i,j} + \delta_{i,j-1} \quad (\text{mod-}2) \quad \text{for} \quad 1 \le j \le n, \quad 1 \le i \le n-1$$

$$h_{n,j} = \delta_{n,j} + b_{j-1} \quad (\text{mod-}2) \quad \text{for} \quad 1 \le j \le n$$

$$\left.\begin{array}{c}\\\\\\\\\\\end{array}\right\} \tag{B-43}$$

and Eq. B-41 becomes

$$V_{i-1}(j) = H V_i(j) \qquad (\text{mod-}2) \tag{B-44}$$

If H is nonsingular then its inverse exists. The determinate of a matrix is equal to the constant term of the characteristic polynomial of the matrix (see Ref. 3, p. 87). The characteristic polynomial of H, $h(\xi)$, is found as follows; let

$$\psi = \xi + 1$$

then by definition

$$h(\xi) = |H + \xi I| \qquad (\text{mod-}2)$$

$$= |C_f + (\xi + 1) I| \qquad (\text{mod-}2)$$

$$= |C_f + \psi I| \qquad (\text{mod-}2)$$

$$= \sum_{i=0}^{n} b_i \psi^i \qquad (\text{mod-}2)$$

$$= \sum_{i=0}^{n} b_i (\xi + 1)^i \qquad (\text{mod-}2)$$

Applying Eq. 118, this becomes

$$h(\xi) = \sum_{i=0}^{n} b_i \sum_{k=0}^{i} (d_k)_i \, \xi^k \quad (\text{mod-2}) \qquad (\text{B-45})$$

Interchanging summations, Eq. B-45 can be written as

$$h(\xi) = \sum_{k=0}^{n} \left[\sum_{i=k}^{n} (d_k)_i \, b_i \right] \xi^k \quad (\text{mod-2})$$

From Eq. 150,

$$c_{n-k} = \sum_{i=k}^{n} (d_k)_i \, b_i \quad (\text{mod-2})$$

and the characteristic polynomial of H becomes

$$h(\xi) = \sum_{k=0}^{n} c_{n-k} \, \xi^k = c_n + c_{n-1} \xi + c_{n-2} \xi^2 + \ldots + c_0 \xi^n \quad (\text{mod-2}) \qquad (\text{B-46})$$

The determinant of H, $|H|$, is therefore

$$|H| = c_n \quad (\text{mod-2})$$

and H has in inverse, H^{-1}, if and only if $c_n = 1$.

Whenever $c_n = 1$ in the SCRG or equivalently, from Eq. 150 $\sum_{i=0}^{n} b_i = 1 \ (\text{mod-2})$ define a matrix G as follows

$$G = [g_{i,j}]_{n \times n}$$

where

$$
\left.
\begin{aligned}
g_{i,j} &= 1 + \sum_{k=0}^{j-1} b_k \quad (\text{mod-2}) \quad \text{for} \quad i \le j \\
&= \sum_{k=0}^{j-1} b_k \quad (\text{mod-2}) \quad \text{for} \quad i > j
\end{aligned}
\right\} \qquad (\text{B-47})
$$

It will now be shown that G, in the above equation, is the inverse of H.

Consider the matrix product

$$H \cdot G = [h_{i,j}]_{n \times n} \cdot [g_{i,j}]_{n \times n} = [t_{i,j}]_{n \times n} \quad (\text{mod-2})$$

$$t_{i,j} = \sum_{m=1}^{n} h_{i,m} \, g_{m,j} \quad (\text{mod-2})$$

For $1 \leq i \leq n-1$, all j

$$t_{i,j} = \sum_{m=1}^{n} [\delta_{i,m} + \delta_{i,m-1}] \, g_{m,j} \qquad (\text{mod-}2)$$

$$= g_{i,j} + g_{i+1,j} \qquad (\text{mod-}2)$$

when $j > i$ this becomes

$$t_{i,j} = \left(1 + \sum_{k=0}^{j-1} b_k\right) + \left(1 + \sum_{k=0}^{j-1} b_k\right) = 0 \qquad (\text{mod-}2)$$

when $j = i$ this becomes

$$t_{i,i} = 1 + \sum_{k=0}^{i-1} b_k + \sum_{k=0}^{i-1} b_k = 1 \qquad (\text{mod-}2)$$

and when $j < i$, it becomes

$$t_{i,j} = \sum_{k=0}^{j-1} b_k + \sum_{k=0}^{j-1} b_k = 0 \qquad (\text{mod-}2)$$

so for $1 \leq i \leq n-1$, all j

$$t_{i,j} = 1 \text{ when } i = j$$

$$= 0 \text{ otherwise}$$

For $i = n$

$$t_{n,j} = \sum_{m=1}^{n} h_{n,m} \, g_{m,j} \qquad (\text{mod-}2)$$

$$= \sum_{m=1}^{n} [\delta_{n,m} + b_{m-1}] \, g_{m,j} = g_{n,j} + \sum_{m=1}^{n} b_{m-1} \, g_{m,j} \qquad (\text{mod-}2)$$

when $j \leq n-1$ this becomes

$$t_{n,j} = \sum_{k=0}^{j-1} b_k + \sum_{m=1}^{j} b_{m-1} \left[1 + \sum_{k=0}^{j-1} b_k\right] + \sum_{m=j+1}^{n} b_{m-1} \sum_{k=0}^{j-1} b_k \qquad (\text{mod-}2)$$

$$= \sum_{k=0}^{j-1} b_k + \sum_{m=1}^{j} b_{m-1} + \sum_{m=1}^{j} b_{m-1} \sum_{k=0}^{j-1} b_k + \sum_{m=j+1}^{n} b_{m-1} \sum_{k=0}^{j-1} b_k \qquad (\text{mod-}2)$$

$$= \sum_{k=0}^{j-1} b_k + \sum_{k=0}^{j-1} b_k + \sum_{m=1}^{n} b_{m-1} \sum_{k=0}^{j-1} b_k \qquad \text{(mod-2)}$$

$$= \sum_{m=0}^{n-1} b_m \sum_{k=0}^{j-1} b_k = \sum_{k=0}^{j-1} b_k \sum_{m=0}^{n-1} b_m \qquad \text{(mod-2)} \qquad \text{(B-48)}$$

From the definition of the characteristic polynomial, an $n \times n$ matrix has $b_n \equiv 1$. In addition for the SCRG, c_n has been assumed 1 which implies

$$\sum_{i=0}^{n} b_i = b_n + \sum_{i=0}^{n-1} b_i = 1 + \sum_{i=0}^{n-1} b_i = 1 \qquad \text{(mod-2)}$$

or

$$\sum_{i=0}^{n-1} b_i = 0 \qquad \text{(mod-2)}$$

Thus Eq. B-48 is equal to zero.

For $i = j = n$

$$t_{n,n} = \sum_{m=1}^{n} h_{n,m} \, g_{m,n} \qquad \text{(mod-2)}$$

$$= \sum_{m=1}^{n} (\delta_{n,m} + b_{m-1}) \left(1 + \sum_{k=0}^{n-1} b_k \right) \qquad \text{(mod-2)}$$

$$= \sum_{m=1}^{n} (\delta_{n,m} + b_{m-1}) \qquad \text{(mod-2)}$$

$$= 1 + \sum_{m=1}^{n} b_{m-1} \qquad \text{(mod-2)}$$

$$= 1 + \sum_{m=0}^{n-1} b_m \qquad \text{(mod-2)}$$

$$= 1 \qquad \text{(mod-2)}$$

Summarizing,

$$t_{i,j} = 1 \text{ when } i = j$$

$$= 0 \text{ when } i \neq j$$

153

and

$$H \cdot G = [t_{i,j}]_{n \times n} = I \quad (\text{mod-2})$$

Therefore, when $c_n = 1$

$$G = H^{-1} \qquad (\text{B-49})$$

and from Eqs. B-44 and B-49

$$V_i(j) = G \, V_{i-1}(j) \quad (\text{mod-2}) \qquad (\text{B-50})$$

The characteristic polynomial of G will be found for the sake of completeness. Let A be any non-singular n x n matrix with characteristic polynomial

$$f(\xi) = |A - \xi I| = \sum_{i=0}^{n} b_i \, \xi^i$$

then it can be shown that the characteristic polynomial of A^{-1} is given by

$$f_{-1}(\xi) = |A^{-1} - \xi I| = (-1)^n b_0^{-1} \sum_{i=0}^{n} b_{n-i} \, \xi^i$$

In mod-2 arithmetic -1 and +1 are the same, and if A is non-singular, then

$$b_0^{-1} = |A|^{-1} = |A| = 1 \quad (\text{mod-2})$$

so

$$f_{-1}(\xi) = \sum_{i=0}^{n} b_{n-i} \, \xi^i \quad (\text{mod-2})$$

and we see that $f_{-1}(\xi)$ is the reverse of $f(\xi)$. Applying this result to the G and H matrices we get the characteristic polynomial of G

$$g(\xi) = |G + \xi I| = \sum_{i=0}^{n} c_i \, \xi^i \quad (\text{mod-2}) \qquad (\text{B-51})$$

154

<u>Theorem 8:</u>

Consider an n-stage SCRG for which $c_n = 1$ and $\sum_{i=0}^{n} c_i = 1$, with

a characteristic polynomial, $f(\xi)$, which is factorable. If any stage

of the SCRG is producing a sequence corresponding to a polynomial

of degree less than n, $f'(\xi)$, where $f(\xi) = f''(\xi) f'(\xi)$, then the se-

quences from every stage of the generator correspond to the same

polynomial $f'(\xi)$.

<u>Proof</u>

Let $X_i(j)$ denote the sequence produced by the i-th stage of the SCRG. Assume

that $X_i(j)$ obeys the sequence law associated with one of the factors, $f'(\xi)$, of the charac-

teristic polynomial $f(\xi)$. From Eq. 173

$$X_{i-1}(j) = X_i(j) + X_i(j+1) \qquad (\text{mod-}2)$$

and from Theorem 1, since $X_i(j)$ and $X_i(j+1)$ obey the same sequence law (they are shifted

versions of the same sequence), their sum, $X_{i-1}(j)$, obeys the same sequence law.

Similarly, $X_m(j)$, $m < i$, obeys the sequence law associated with $f'(\xi)$.

Since $c_n = 1$, the G matrix defined by Eq. 172 exists and Eq. 171 holds, that

is

$$V_{i+1}(j) = G V_i(j) \qquad (\text{mod-}2)$$

or equivalently

$$u_{i+1}(j) = \sum_{k=1}^{n} g_{1,k} u_i(j+k-1) \qquad (\text{mod-}2)$$

which leads to

$$X_{i+1}(j) = \sum_{k=1}^{n} g_{1,k} X_i(j+k-1) \qquad (\text{mod-}2) \tag{B-52}$$

Applying Theorem 1 to Eq. B-52, $X_{i+1}(j)$ obeys the same sequence law that $X_i(j)$ obeys.

Similarly $X_m(j)$ for $i < m \leq n$ obeys the sequence law associated with the factor $f'(\xi)$.

Theorem 8 is obtained by combining these two results.

Before considering Theorem 9, the following lemma will be established.

155

If an n-stage SCRG contains "0's" in p consecutive stages (say Stages m through m+p-1) at any time j, then the output sequence from Stage m+p-1 starting at time j will contain p consecutive "0's."

Proof

From Eq. 111 for an SCRG

$$u_{i+1}(j+1) = u_{i+1}(j) + u_i(j) \quad (\text{mod-2}) \quad \text{for} \quad i \geq 1$$

Given that

$$u_{m+k}(j) = 0 \quad \text{for} \quad 0 \leq k \leq p-1 \tag{B-53}$$

then

$$u_{m+1+k}(j+1) = u_{m+k+1}(j) + u_{m+k}(j) \quad (\text{mod-2})$$
$$= 0 \quad \text{for} \quad 0 \leq k \leq p-2 \tag{B-54}$$

Suppose that for some value of q

$$u_{m+q+k}(j+q) = 0 \quad \text{for} \quad 0 \leq k \leq p-q-1, \quad q \leq p-2 \tag{B-55}$$

then for $0 \leq k \leq p-q-2, \quad q+1 \leq p-1$

$$u_{m+q+1+k}(j+q+1) = u_{m+q+k}(j+q) + u_{m+q+k+1}(j+q) \quad (\text{mod-2})$$
$$= 0 + 0$$
$$= 0 \tag{B-56}$$

From inspection of Eqs. B-53 and B-54, Eq. B-55 is true for q = 0, and q = 1. Also by Eq. B-56, if Eq. B-55 is true for any value of q such that $q \leq p-2$ then it is true for the next larger value of q, thus by induction

$$u_{m+q+k}(j+q) = 0 \quad \text{for} \quad 0 \leq k \leq p-q-1, \quad q \leq p-1 \tag{B-57}$$

In particular, when k = p-q-1

$$u_{m+p-1}(j+q) = 0 \quad \text{for} \quad 0 \leq q \leq p-1 \tag{B-58}$$

<u>Theorem 9</u>:

Consider an n-stage SCRG with $c_n = 1$ and $\sum_{i=0}^{n} c_i = 1$, with a characteristic polynomial, $f(\xi)$, which is factorable, $f(\xi) = f'(\xi), \ldots, f''(\xi)$.
If any p consecutive stages of the generator $(p \leq n)$ contain zeros at any time j, then none of the sequences being produced by the generator can be produced by a generator of p or fewer stages, unless every stage is producing all zeros.

<u>Proof</u>

From the above lemma, if p consecutive stages of the generator contain zeros at some time j, then the output sequence from one of the stages will contain p consecutive "0's." It is impossible to generate a linear sequence, using a p-stage generator, that contains p zeros except the all-zero sequence. If the i-th stage were producing all zeros then every stage would be producing all zeros because, by repeated application of Eqs. 167 and 171,

$$V_{i-k}(j) = H^k V_i(j) = 0 \quad (\text{mod-}2)$$

and

$$V_{i+k}(j) = G^k V_i(j) = 0 \quad (\text{mod-}2)$$

If this is not true, then some stage of the SCRG is producing a nontrivial sequence which cannot be generated by a generator of p stages or less. Theorem 9 states that if one stage of an SCRG is producing a sequence that can be produced by an m-stage generator, then every stage of the generator is producing a sequence which can be produced by the same m-stage generator. Therefore, m must be greater than p.

<u>Theorem 10</u>:

Consider an n-stage SSRG and an n-stage SCRG which have the same <u>feedback</u> (not characteristic) equation. Let $Y_i(j)$ represent the content vector of the SSRG at time j, and let $U(j)$ represent the content vector of the SCRG at time j. If $U(K) = Y(K)$ at some time K, then

$$[U(K), U(K+1), \ldots, U(K+n-1)] = [Y(K), Y(K+1), \ldots, Y(K+n-1)] \cdot R_2 \quad (\text{mod-}2)$$

and

$$[Y(K), Y(K+1), \ldots, Y(K+n-1)] = [U(K), U(K+1), \ldots, U(K+n-1)] \cdot R_2 \quad (\text{mod-}2)$$

157

<u>Proof</u>

Let A_s be the "A" matrix for the SSRG and let A_c be the A matrix for the SCRG. If both generators have the same feedback equation, then

$$A_c = A_s + I \quad (\text{mod-}2)$$

Applying Eq. 118

$$A_c^k = (A_s + I)^k \quad (\text{mod-}2) \quad \text{for} \quad k \geq 0$$

$$= \sum_{i=0}^{k} (d_i)_k A_s^i \quad (\text{mod-}2)$$

If at some time K

$$U(K) = Y(K)$$

then

$$U(K + k) = A_c^k U(K) \quad (\text{mod-}2)$$

$$= A_c^k Y(K) \quad (\text{mod-}2)$$

$$= \sum_{i=0}^{k} (d_i)_k A_s^i Y(K) \quad (\text{mod-}2)$$

$$= \sum_{i=0}^{k} (d_i)_k Y(K + i) \quad (\text{mod-}2)$$

or

$$u_p(K+k) = \sum_{i=0}^{k} y_p(K+i) (d_i)_k \quad (\text{mod-}2) \quad \text{for } k \geq 0 \qquad (\text{B-}59)$$

In matrix form Eq. B-59 becomes for $0 \leq k \leq n-1$

$$\begin{bmatrix} u_1(K) & u_1(K+1) & \cdots & u_1(K+n-1) \\ u_2(K) & u_2(K+1) & \cdots & u_2(K+n-1) \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ u_{n-1}(K) & u_{n-1}(K+1) & \cdots & u_{n-1}(K+n-1) \\ u_n(K) & u_n(K+1) & \cdots & u_n(K+n-1) \end{bmatrix} =$$

$$\begin{bmatrix} y_1(K) & y_1(K+1) & \cdots & y_1(K+n-1) \\ y_2(K) & y_2(K+1) & \cdots & y_2(K+n-1) \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ y_{n-1}(K) & y_{n-1}(K+1) & \cdots & y_{n-1}(K+n-1) \\ y_n(K) & y_n(K+1) & \cdots & y_n(K+n-1) \end{bmatrix} \cdot \begin{bmatrix} (d_0)_0 & (d_0)_1 & \cdots & (d_0)_{n-2} & (d_0)_{n-1} \\ 0 & (d_1)_1 & \cdots & (d_1)_{n-2} & (d_1)_{n-1} \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ 0 & 0 & \cdots & (d_{n-2})_{n-2} & (d_{n-2})_{n-1} \\ 0 & 0 & \cdots & 0 & (d_{n-1})_{n-1} \end{bmatrix} \quad (\text{mod-2})$$

$$(\text{B-60})$$

The matrix on the far right in Eq. B-60 is recognized as the R_2 matrix, thus

$$[U(K), U(K+1), \ldots, U(K+n-1)] = [Y(K), Y(K+1), \ldots, Y(K+n-1)] \cdot R_2 \quad (\text{mod-2})$$

and since $R_2^{-1} = R_2$

$$[Y(K), Y(K+1), \ldots, Y(K+n-1)] = [U(K), U(K+1), \ldots, U(K+n-1)] \cdot R_2 \quad (\text{mod-2})$$

159

APPENDIX C

These theorems were presented without proof in Section 6. They deal with the modular-complement-register generator.

Theorem 11:

Given an n-stage MCRG with a factorable characteristic polynomial

$$f(\xi) \;=\; f'(\xi),\; f''(\xi)\; \ldots\; f'''(\xi) \qquad (\text{mod-2})$$

The sequences produced by each stage of the MCRG follow the same

sequence law as is followed by the sequence produced by the last stage.

(Note: some stages may produce the all-zero sequence.)

Proof

Let $X_i(j)$ be the sequence produced by the i-th stage with time reference j. For an MCRG

$$u_{i-1}(j) \;=\; u_i(j) \;+\; u_i(j+1) \;+\; c_{i-1}\, u_n(j) \qquad (\text{mod-2})$$

or

$$X_{i-1}(j) \;=\; X_i(j) + X_i(j+1) + c_{i-1}\, X_n(j) \qquad (\text{mod-2})$$

Let $i = n$, then

$$X_{n-1}(j) \;=\; (1+c_{n-1})\, X_n(j) + X_n(j+1) \qquad (\text{mod-2})$$

By Theorem 1, $X_{n-1}(j)$ obeys the same sequence law that $X_n(j)$ obeys. Suppose that for some value of k, $2 \leq k \leq n$, that $X_k(j)$ obeys the same sequence law as $X_n(j)$ obeys, then

$$X_{k-1}(j) \;=\; X_k(j) + X_k(j+1) + c_{k-1}\, X_n(j) \quad (\text{mod-2})$$

and by Theorem 1, $X_{k-1}(j)$ follows the same sequence law that $X_n(j)$ follows.

160

We have seen that $X_k(j)$ follows the sequence law that $X_n(j)$ follows when $k = n-1$ and it is obviously true for $k = n$. Also, if $X_k(j)$ obeys the law of $X_n(j)$, then $X_{k-1}(j)$ obeys the law of $X_n(j)$. Therefore, by induction, for all k such that $1 \leq k \leq n$, $X_k(j)$ follows the same sequence law that $X_n(j)$ follows.

Theorem 12:

Given an n-stage MCRG; if $u_1(j) = 1$ and $u_i(j) = 0$ for $2 \leq i \leq n$ at some time j, then

$$u_i(j+k) = (d_{i-1})_k \quad \text{for} \quad 1 \leq i \leq k+1, \quad 0 \leq k \leq n-1$$

and

$$u_i(j+k) = 0 \quad \text{for} \quad k+2 \leq i \leq n, \quad 0 \leq k \leq n-2$$

(C-1)

Proof

From Eq. 187 for an MCRG

$$u_1(p+1) = u_1(p) + c_0 u_n(p) \qquad \text{(mod-2)}$$

$$u_i(p+1) = u_{i-1}(p) + u_i(p) + c_{i-1} u_n(p) \qquad \text{(mod-2)}$$

By hypothesis

$$u_i(j) = 1 = (d_0)_0 \quad \text{for} \quad i = 1$$

$$= 0 \quad \text{for} \quad 2 \leq i \leq n$$

Therefore

$$u_1(j+1) = u_1(j) + c_0 u_n(j) \qquad \text{(mod-2)}$$

$$= 1 = (d_0)_1$$

Similarly

$$u_2(j+1) = u_1(j) + u_2(j) + c_1 u_n(j) \qquad \text{(mod-2)}$$

$$= 1 = (d_1)_1$$

161

and

$$u_i(j+1) = u_{i-1}(j) + u_i(j) + c_{i-1} u_n(j) \quad \text{(mod-2)}$$

$$= 0 \quad \text{for} \quad 3 \leq i \leq n$$

Thus for $k = 0, 1$

$$u_i(j+k) = (d_{i-1})_k \quad \text{for} \quad 1 \leq i \leq k+1$$

$$= 0 \qquad \text{for} \quad k+2 \leq i \leq n$$

$$\left.\right\} \quad \text{(C-2)}$$

Assume that Eq. C-1 is true for some aribtrary value of k such that $1 \leq k \leq n-2$, then

$$u_1(j+k+1) = u_1(j+k) + c_0 u_n(j+k) \quad \text{(mod-2)}$$

$$= (d_0)_k + 0$$

$$= (d_0)_{k+1}$$

$$u_i(j+k+1) = u_{i-1}(j+k) + u_i(j+k) + c_{i-1} u_n(j+k) \quad \text{(mod-2)}$$

$$= (d_{i-2})_k + (d_{i-1})_k \quad \text{(mod-2)}$$

$$= (d_{i-1})_{k+1} \quad \text{for} \quad 2 \leq i \leq k+1$$

$$u_{k+2}(j+k+1) = u_{k+1}(j+k) + u_{k+2}(j+k) + c_{k+1} u_n(j+k) \quad \text{(mod-2)}$$

$$= (d_k)_k$$

$$= (d_{k+1})_{k+1}$$

$$u_i(j+k+1) = u_{i-1}(j+k) + u_i(j+k) + c_{i-1} u_n(j+k) \quad \text{(mod-2)}$$

$$= 0 \quad \text{for} \quad k+3 \leq i \leq n$$

so

$$u_i(j+k+1) = (d_{i-1})_{k+1} \quad \text{for} \quad 1 \leq i \leq (k+1) + 1$$

$$= 0 \quad \text{for} \quad (k+1) + 2 \leq i \leq n \quad \text{if} \quad k+1 \leq n-2$$

If Eq. C-1 is true for any particular value of k such that $1 \leq k \leq n-2$, then it is true for the next larger value of k. Equation C-2 shows that Eq. C-1 is true for $k = 0, 1$, thus by induction Eq. C-1 is true for all k such that $0 \leq k \leq n-1$.

This theorem, dealing with the Jacobian-hybrid generator, was presented without proof in Section 7.

<u>Theorem 13</u>:

If an n-stage JHG is initially loaded with $U(j) = E_1(0)$, that is

$$u_1(j) = 1$$

$$u_i(j) = 0 \quad \text{for} \quad 2 \leq i \leq n$$

then

$$u_k(j+k-1) = 1 \quad \text{for} \quad 1 \leq k \leq n$$

and

$$u_i(j+k-1) = 0 \quad \text{for} \quad 2 \leq k+1 \leq i \leq n$$

<u>Proof</u>

From Eq. 229

$$u_i(j+k) = u_{i-1}(j+k-1) + c_i u_i(j+k-1) + u_{i+1}(j+k-1) \quad (\text{mod-2}) \quad 2 \leq i \leq n-1$$

$$u_n(j+k) = u_{n-1}(j+k-1) + c_n u_n(j+k-1) \quad (\text{mod-2})$$

Assume for some arbitrary k such that $1 \leq k \leq n-2$ that

$$u_k(j+k-1) = 1$$

and

$$u_i(j+k-1) = 0$$

(D-1)

where $k < i \leq n$ then

$$u_{k+1}(j+k) = u_k(j+k-1) + c_{k+1} u_{k+1}(j+k-1) + u_{k+2}(j+k-1) \quad (\text{mod-2})$$

$$= 1 \tag{D-2}$$

and

$$u_i(j+k) = u_{i-1}(j+k-1) + c_i u_i(j+k-1) + u_{i+1}(j+k-1) \quad (\text{mod-2})$$

$$= 0 \quad \text{for} \quad k+1 < i \leq n-1 \tag{D-3}$$

$$u_n(j+k) = u_{n-1}(j+k-1) + c_n u_n(j+k-1) \quad (\text{mod-2})$$

$$= 0 \tag{D-4}$$

By hypothesis, Eq. D-1 is true for $k = 1$. From Eqs. D-2, D-3, and D-4, if Eq. D-1 is true for any arbitrary value of k such that $1 \leq k \leq n-2$, then Eq. D-1 is valid for the next larger value of k. Thus by induction

$$u_k(j+k-1) = 1$$

and

$$u_i(j+k-1) = 0 \quad \text{for} \quad 1 \leq k \leq n-1 \tag{D-5}$$

and

$$k+1 \leq i \leq n$$

From Eq. D-5,

$$u_n(j+n-1) = u_{n-1}(j+n-2) + c_n u_n(j+n-2) \quad (\text{mod-2})$$

$$= 1$$

Therefore

$$u_k(j+k-1) = 1 \quad \text{for} \quad 1 \leq k \leq n$$

$$u_i(j+k-1) = 0 \quad \text{for} \quad 1 \leq k \leq n-1 \quad \text{and} \quad k+1 \leq i \leq n$$

REFERENCES

1. Birdsall, T. G.   Ristenbatt, M. P.   Introduction to linear shift-register generated sequences. Technical Report No. 90. (2262-189-T). Ann Arbor: Cooley Electronics Laboratory, The University of Michigan, October, 1958.

2. Birdsall, T. G.   Hoopes, C.   Extensions of linear shift-register generated sequences. (U) Technical Report No. 113. (2899-46-T). Ann Arbor: Cooley Electronics Laboratory, The University of Michigan, February, 1962. (SECRET).

3. Nering, E. D.   Linear algebra and matrix theory. New York: Wiley, 1964.

4. Feller, W.   An introduction to probability theory and its applications. Vol. L New York: Wiley, 1957. (2nd Ed.).

5. Peterson, W.W.   Error-correcting codes. New York: Wiley, 1961.

No. of
Copies

No. of
Copies

1   Office of Assistant Secretary of
       Defense
       (R&E) Room 3E1065
       The Pentagon
       Washington, D. C. 2031
       ATTN: Technical Library

2-3   Chief of Research and Development
       Department of the Army
       Washington, D. C. 20310

4   Commanding General
       U. S. Army Security Agency
       Arlington Hall Station
       Arlington, Virginia 22212
       ATTN: ACofS, G3

5   Commanding General
       U. S. Army Security Agency
       Arlington Hall Station
       Arlington, Virginia 22212
       ATTN: ACofS, G4

6   Deputy President
       U. S. Army Security Agency Board
       Arlington Hall Station
       Arlington, Virginia 22212

7-10   Commanding General
       U. S. Army Security Agency
       Arlington Hall Station
       Arlington, Virginia 22212
       ATTN: IADEV-SR

11   Commanding General
       U. S. Army Security Agency
       Arlington Hall Station
       Arlington, Virginia 22212
       ATTN: IACON

12   USASA Technical Representative
       U. S. Army Electronics
         Laboratories
       Evans Area
       Belmar, New Jersey 07703

13-15   Director
       U. S. Army Electronics
         Laboratories
       Fort Monmouth, New Jersey 07703
       ATTN: AMSEL-RD-SEE

16   Commanding General
       U. S. Army Materiel Command
       Washington, D. C. 20315
       ATTN: R&D Directorate

17   Chief
       U. S. Army Electronics
         Laboratories
       Mountain View Office
       P. O. Box 205
       Mountain View, California

18   Director
       U. S. Army Electronics
         Laboratories
       Fort Monmouth, New Jersey 07703
       ATTN: AMSEL-RD-ADO-RHA

19   Director
       U. S. Army Electronics
         Laboratories
       Fort Monmouth, New Jersey 07703
       ATTN: AMSEL-RD-ADO-ADT

20   Director
       U. S. Army Electronics
         Laboratories
       Fort Monmouth, New Jersey 07703
       ATTN: AMSEL-RD-DR

21-40   Commander
       Defense Documentation Center
       Cameron Station, Bldg. 5
       Alexandria, Virginia 20315
       ATTN: TISIA

41   Commanding General
       U. S. Army Electronics Command
       Fort Monmouth, New Jersey 07703
       ATTN: AMSEL-EW

42   Technical Director
       U. S. Army Electronics Command
       Fort Monmouth, New Jersey 07703

43-47   Director
       National Security Agency
       Fort George C. Meade, Maryland
                         20755
       ATTN: R-3, Mr. M. H. Klein

No. of
Copies

No. of
Copies

48   Commanding Officer
52d USASA Special Operations
     Command
Fort Huachuca, Arizona   85613

51   Dr. T. W. Butler, Director
Cooley Electronics Laboratory
The University of Michigan
Ann Arbor, Michigan

49   Director
U. S. Army Electronics L
     Laboratories
Fort Monmouth, New Jersey   07703
ATTN: AMSEL-RD-SE

52-70   Cooley Electronics Laboratory
The University of Michigan
Ann Arbor, Michigan

50   Commander
Rome Air Development Center
Griffis Air Force Base, New York
ATTN:EMIAP

71   Remote Area Conflict Information
     Center
Battelle Memorial Institute
505 King Avenue
Columbus, Ohio   43201

DOCUMENT CONTROL DATA - R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author)	2a. REPORT SECURITY CLASSIFICATION
Cooley Electronics Laboratory The University of Michigan Ann Arbor, Michigan	Unclassified
	2b. GROUP

3. REPORT TITLE

Study of Linear Sequence Generators

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*

Technical Report No. 165

5. AUTHOR(S) *(Last name, first name, initial)*

C. C. Hoopes
R. N. Randall

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
June 1966	181	5

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
DA-28-043 AMC-00080(E)	6576-4-T
b. PROJECT NO. 6576	
c.	9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*
d.	Technical Report 165

10. AVAILABILITY/LIMITATION NOTICES

This document is subject to special export controls and each transmittal to foreign nationals or foreign givernments may be made only with prior approval of CG, U.S. Army Electronics Command, Fort Monmouth, N. J. ATTN: AMSEL-WL-C

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	Commanding General U. S. Army Electronics Command Fort Monmouth, New Jersey AMSEL-WL-C

13. ABSTRACT

This report treats techniques for generating linear binary sequences. The basic properties of sequence generators, maximal sequences, and non maximal sequences are reviewed. Five specific types of generators, each representing a "canonical form," are considered. Two forms of shift-register generators are studied: the simple-shift-register generator and the modular-shift-register generator. Two forms of complement-register generators are considered: the simple-complement-register generator and the modular-complement-register generator. A hybrid generator consisting of both shift and complement stages is discussed. Included in the discussion for each generator are: (1) the relationship between the characteristic polynomial and the feedback connections, (2) the relationship between sequences produced by different stages of the same generator, (3) the initial loading required for the generator to produce a particular n-tuple from the output stage, and (4) an output adder technique to obtain the desired starting conditions for a sequence obeying the law of the generator.

The advantages and disadvantages of each of the five generators are given. Also tables of equivalent generators for all maximal characteristic polynomials of degree $2 \leq n \leq 12$ are included.

Matrix theory is used throughout the report to prove necessary theorems, and it is used in the development of mathematical descriptions of the generators.

DD FORM 1 JAN 64 **1473**

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Algebra						
Binary Arithmetic						
Computer Logic						
Determinants						
Equations						
Factor Analysis						
Feedback Generators						
Generators						
Equivalent Generators						
Linear Sequences						
Mathematical Analysis						
Matrix Algebra						
Polynomials						

INSTRUCTIONS

1. ORIGINATING ACTIVITY: Enter the name and address of the contractor, subcontractor, grantee, Department of Defense activity or other organization (corporate author) issuing the report.

2a. REPORT SECURITY CLASSIFICATION: Enter the overall security classification of the report. Indicate whether "Restricted Data" is included. Marking is to be in accordance with appropriate security regulations.

2b. GROUP: Automatic downgrading is specified in DoD Directive 5200.10 and Armed Forces Industrial Manual. Enter the group number. Also, when applicable, show that optional markings have been used for Group 3 and Group 4 as authorized.

3. REPORT TITLE: Enter the complete report title in all capital letters. Titles in all cases should be unclassified. If a meaningful title cannot be selected without classification, show title classification in all capitals in parenthesis immediately following the title.

4. DESCRIPTIVE NOTES: If appropriate, enter the type of report, e.g., interim, progress, summary, annual, or final. Give the inclusive dates when a specific reporting period is covered.

5. AUTHOR(S): Enter the name(s) of author(s) as shown on or in the report. Enter last name, first name, middle initial. If military, show rank and branch of service. The name of the principal author is an absolute minimum requirement.

6. REPORT DATE: Enter the date of the report as day, month, year; or month, year. If more than one date appears on the report, use date of publication.

7a. TOTAL NUMBER OF PAGES: The total page count should follow normal pagination procedures, i.e., enter the number of pages containing information.

7b. NUMBER OF REFERENCES: Enter the total number of references cited in the report.

8a. CONTRACT OR GRANT NUMBER: If appropriate, enter the applicable number of the contract or grant under which the report was written.

8b, 8c, & 8d. PROJECT NUMBER: Enter the appropriate military department identification, such as project number, subproject number, system numbers, task number, etc.

9a. ORIGINATOR'S REPORT NUMBER(S): Enter the official report number by which the document will be identified and controlled by the originating activity. This number must be unique to this report.

9b. OTHER REPORT NUMBER(S): If the report has been assigned any other report numbers (either by the originator or by the sponsor), also enter this number(s).

10. AVAILABILITY/LIMITATION NOTICES: Enter any limitations on further dissemination of the report, other than those imposed by security classification, using standard statements such as:

(1) "Qualified requesters may obtain copies of this report from DDC."

(2) "Foreign announcement and dissemination of this report by DDC is not authorized."

(3) "U. S. Government agencies may obtain copies of this report directly from DDC. Other qualified DDC users shall request through

_____ ."

(4) "U. S. military agencies may obtain copies of this report directly from DDC. Other qualified users shall request through

_____ ."

(5) "All distribution of this report is controlled. Qualified DDC users shall request through

_____ ."

If the report has been furnished to the Office of Technical Services, Department of Commerce, for sale to the public, indicate this fact and enter the price, if known.

11. SUPPLEMENTARY NOTES: Use for additional explanatory notes.

12. SPONSORING MILITARY ACTIVITY: Enter the name of the departmental project office or laboratory sponsoring (paying for) the research and development. Include address.

13. ABSTRACT: Enter an abstract giving a brief and factual summary of the document indicative of the report, even though it may also appear elsewhere in the body of the technical report. If additional space is required, a continuation sheet shall be attached.

It is highly desirable that the abstract of classified reports be unclassified. Each paragraph of the abstract shall end with an indication of the military security classification of the information in the paragraph, represented as (TS), (S), (C), or (U).

There is no limitation on the length of the abstract. However, the suggested length is from 150 to 225 words.

14. KEY WORDS: Key words are technically meaningful terms or short phrases that characterize a report and may be used as index entries for cataloging the report. Key words must be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, militar project code name, geographic location, may be used as key words but will be followed by an indication of technical context. The assignment of links, rules, and weights is optional.