THE UNIVERSITY OF MICHIGAN

INDUSTRY PROGRAM OF THE COLLEGE OF ENGINEERING

# INTRODUCTION TO LINEAR SHIFT-REGISTER GENERATED SEQUENCES

heodore
T. G. Birdsall

M. P. Ristenbatt

This report was originally distributed as Technical Report No. 90 by the Electronic Defense Group, Department of Electrical Engineering, The University of Michigan, under The University of Michigan Research Institute Project 2262. This work was sponsored by the U. S. Army Signal Corps.

November, 1958

IP-338

## TABLE OF CONTENTS

## LIST OF ILLUSTRATIONS

## LIST OF TABLES

## Acknowledgments

The authors wish to express their appreciation to Professor A. B. Macnee for his technical editing of this report and his general technical support. Credit is due to Mr. James Daws for his handling of the experimental work. Finally, we appreciate the cooperation of Dr. Robert Price of Lincoln Laboratories in making available pertinent reports.

# INTRODUCTION TO LINEAR SHIFT-REGISTER GENERATED SEQUENCES

## INTRODUCTION

One of the recent developments in communications equipment has been the use of digital sequences to generate waveforms having certain desired properties. One such application is the Rake System (Ref. 1), developed at M.I.T., Lincoln Laboratories which uses waveforms generated from digital sequences to form the reference signals for a teletype communication system. Either one of two waveforms is broadcast from the transmitter; the receiver, which is generating the exact same sequences, crosscorrelates its internally generated waveforms with the incoming signal to determine which of the two was broadcast. The peculiar advantages of the digitally-generated waveform in this application are that the resulting waveform has a wide bandwidth, the power is nearly uniform throughout the bandwidth, and the autocorrelation function is approximately zero outside of the narrow peak at zero delay.

An application in radar is treated by Siebert (Ref. 2), where the digital sequence is used to modulate the output pulse of a radar. The advantage here is that the traditional compromise between output power and range resolution is offset considerably. The modulating of the output pulse by the digital sequence allows a long pulse to achieve the range resolution of a short one. This means that the position uncertainty is limited by the digit pulse width while the average output power is limited by the total transmitted pulse width.

A digital sequence refers to a succession of binary states; for convenience the binary states are usually regarded as consisting of 0's and 1's. When considering digital sequences it is implied that the digits of the series occur in a known or deterministic manner, as opposed to a "random sequence" in which the binary state at any particular time is determined by probabilistic properties. However, the properties of the digital sequences are similar to random sequences in many respects, and therefore digital sequences are often referred to as "psuedo-random" sequences.

The purpose of this report is to present in an orderly fashion what we regard as the fundamentals concerning the generation and properties of digital sequences. We wish to deal with such questions as the following: For a given number of stages, how many maximal sequences are attainable? What connections of the stages result in these maximally long sequences? What are the auto-correlation properties of both maximal and non-maximal sequences? In pursuing this goal, the mathematical methods for treating digital sequences are elucidated. Since the mathematical treatment of digital sequences involves the use of material that is often not familiar to the engineer, an important goal of this report will be to develop the techniques from the tools generally used by engineers. Most of this report is based on work done with an experimental shift-register and accompanying theoretical work at EDG. The approach is oriented towards the practical viewpoint of dealing with sequences, but the theoretical work necessary to justify conclusions is included. Although the major interest in the past has been in maximal sequences, we shall also consider some structure of non-maximal sequences, which has been noted.

In this report long mathematical proofs are not introduced in the text, but rather assigned to the Appendix. Short proofs and intuitive justifications appear in the text, but all the others are in the Appendix.

In Section 1 the shift-register as a generator of digital sequences is considered, and the shift-register itself is described. A necessary auxiliary topic to this is a short treatment of modulo-two addition, which is used in a shift-register generator (SRG). Also in this section the relations of the SRG to other generators of digital sequences is considered. Section 2 is devoted to the fundamental properties of sequences. The initial discussion of these properties does not require a mathematical formulation of the shift-register operation; this section provides a broad basis which will make the following, more detailed, sections easier to follow.

Section 3 deals with the mathematical formulation of both the shift-register and the sequences that it produces. An important part of this section consists of setting up notations which are necessary to treat this topic. Section 4 then uses these mathematical formulations to deal specifically with maximally long sequences, and Section 5 treats the non-maximal case. In both of these sections the major aim is to exhibit the mathematical structure of the sequences, and of the relations between the sequences.

## SECTION 1. SHIFT REGISTER GENERATION OF BINARY SEQUENCES

A shift-register generator consists essentially 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 the output of the adders are fed back to some other stage of the register so that a single (or multiple) closed loop is 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 the ensuing digital sequence depends on both the feedback connections and on the initial loading (or content) of the shift-register.

Previous to being used to generate digital sequences, the major use of a shift-register was in the arithmetic unit of a digital computer. A shift-register consists of a series of bistable elements with the capability of moving what is in each element to the next element by means of a "shift" pulse (Ref. 3). The general technique for accomplishing this consists of returning each element to the 0 state whenever a shift pulse arrives, and then providing for a delayed signal to arrive from the previous stage (of any element) if the particular previous stage formerly was in the 1 state. The basic block diagram for a shift-register is shown in Figure 1(a). In all future diagrams we shall not show the shift signal path or the delay units, but shall show only the series of bistable elements as indicated in Figure 1(b).

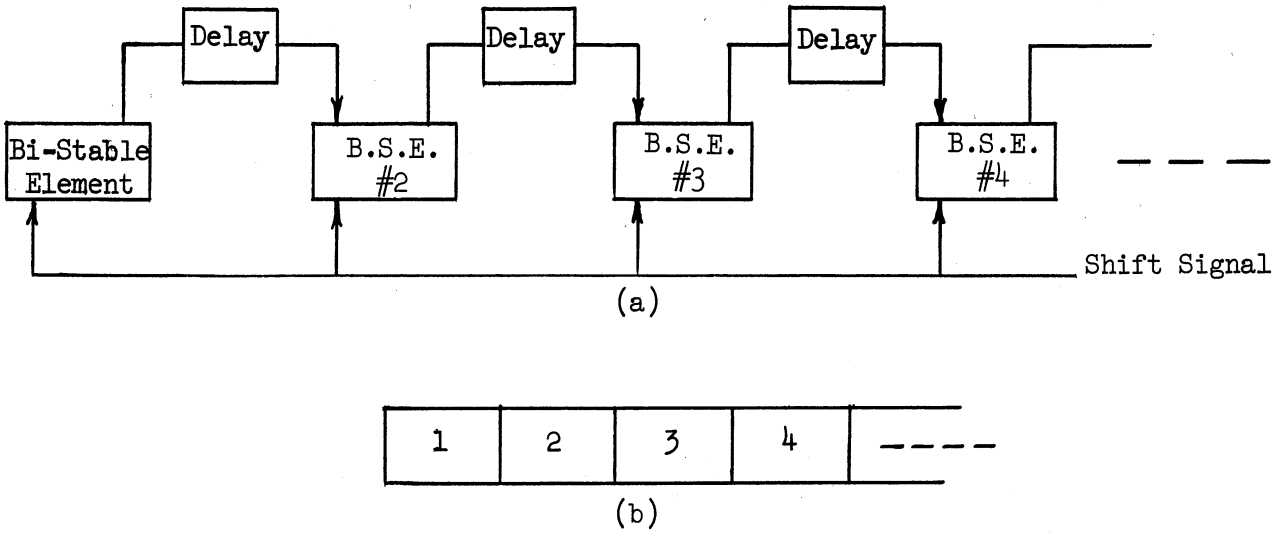


Figure 1. Block Diagram of a Basic Shift-Register

A shift-register is thus a storage unit which moves its stored contents one position for each shift pulse. If such a shift-register has some initial zeros and ones stored in it, as the register is pulsed the output of the last stage will be these stored zeros and ones followed by a string of zeros. However, if the last stage is fed back to the first stage, the output of the last stage will now be periodic-----just the initially stored digits circulating around and around. These two uses of the shift-register are not "shift-register generators," but are storage devices. The object of the "generator" is to produce outputs with periods much longer than the length of the register, but with no external input.

Later, when considering multiple-return generators,' we shall broaden the concept of shift-register to 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 on the connections between the units.

To form a shift-register generator, modulo-two adders are attached to this basic register to form feedback loops. At this point a few comments on modulo-two addition are appropriate. The addition table for modulo-two addition is shown in Figure 2; circuits which operate according to this table are often referred to as "exclusive-or" circuits by computer logicians. It is noted that there is no output when the inputs are alike, and there is an output whenever the inputs are different.

|  | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

Figure 2. Modulo-Two Addition Table

Ordinary binary addition is a combination of modular addition and a carry operation; if one wishes he can view modulo-two addition as ordinary addition written to the base two, where only the least significant digit is recorded.

One of the simplest shift-register generators consists of using one adder along with the basic shift-register. A simple generator is shown in Figure 3, where the numbers in the blocks refer to the bistable elements of the basic shift-register. The output could be taken from any of the stages but we usually think of the output as coming from the last stage of the register.

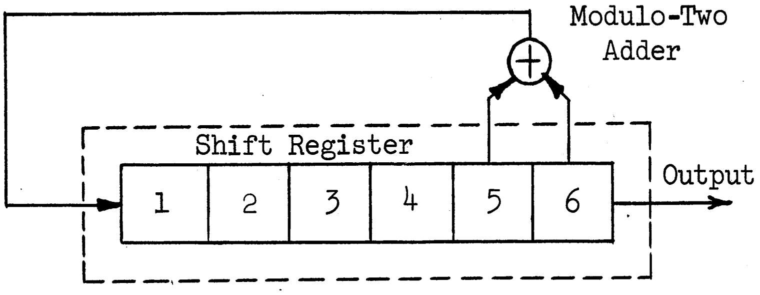


Figure 3. A Simple Shift-Register Generator

To see that this is truly a generator and not just a storage device, consider an initial storage of six ones. The next five inputs will all be zeros since the initial ones will continue to be shifted into both the fifth and sixth stages for five shifts. The total sequence has a period of sixty-three digits (compared to six for storage), and is 11111100000100001100010100 1111010001110010010110111011001101010, repeated over and over.

Although the register elements of Figure 3 are all connected directly to each other, frequently it is useful to think of modulo-two adders as also existing between the elements. In order to produce the same effect as in Figure 3 one input of these additional adders will be grounded. Thus, for purposes of generality, we wish to modify the generator of Figure 3 as depicted in Figure 4. The important idea behind these extra adders is that we could, if we wished, form feedback loops between any stages. Note that, in Figure 4, grounding one input of the adders between stages is the same

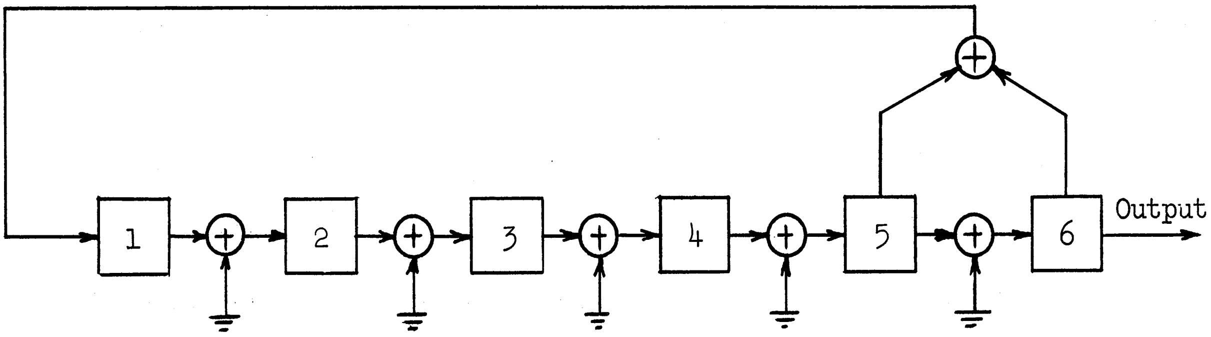


Figure 4. A More General Representation of a Simple Shift-Register, as in Figure 3

thing as connecting the stages directly; that is a general property of modulo-two adders.

We can now distinguish between two types of shift-register generators. If the stages are connected as in both Figures 3 and 4, we shall call the resulting generator a simple shift-register generator. We shall henceforth use the representation of Figure 3 to denote the simple shift-register generator (SSRG). The other type of generator to which we shall refer is called the "multiple-return" generator, and an example of such a generator is shown in Figure 5.

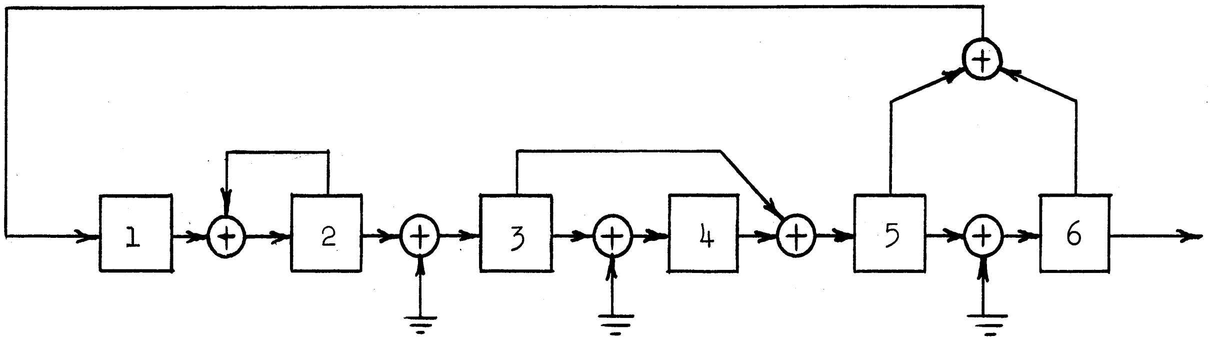


Figure 5. An Example of a Multiple-Return Generator

In the SSRG feedbacks are all returned to a single input. A multiple-return generator will have adder outputs to two or more stage inputs. It is possible in such a generator to have feedforward as well as feedback connections. Since the interstage adders that have one input grounded are superfluous, a better representation of the chosen example is shown in Figure 6. The difference between the simple and the multiple-return generators will appear throughout this report. We shall see that every multiple-return generator (that has no transients) possesses an equivalent simple generator.

Another feature of an SRG concerns the number of feedback taps made from the basic shift-register. In thinking of this we need consider only the simple generator, for the reason that every multi-return generator has a simple

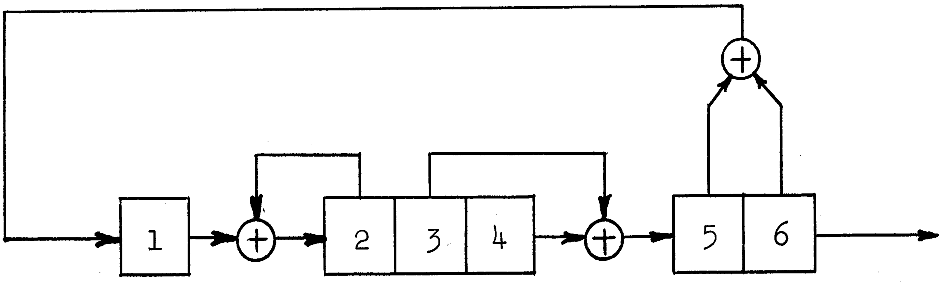
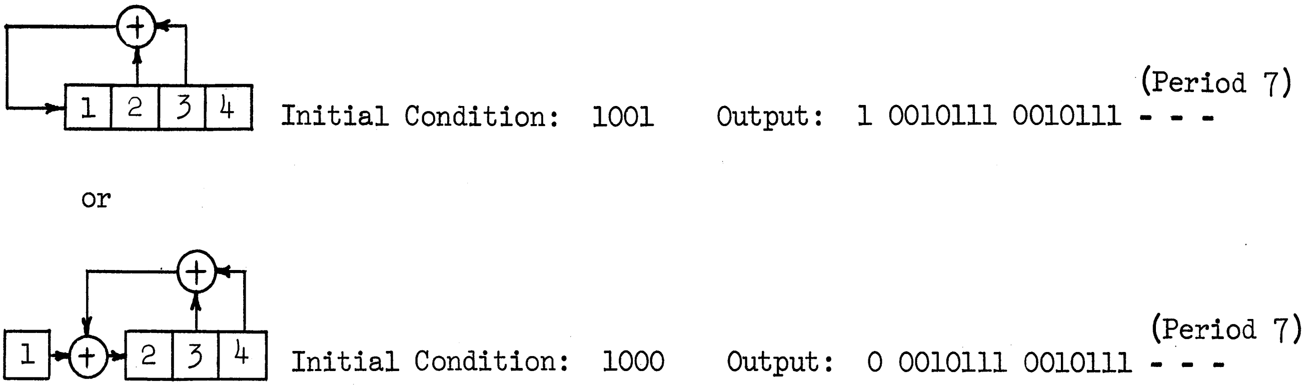


Figure 6. Another representation of the generator of Figure 5

equivalent. If the number of feedback connections (on the simple generator) is an even number then we shall term the resulting generator an "even feedback" generator. All of the examples shown so far are generators of the even feedback type -- in order to ascertain this for the multiple-return case it is necessary first to find the simple equivalent, which will be considered later.

We shall have occasion, later, to exclude generators that have transients in their sequences, and hence it is pertinent to briefly describe them. If an SRG produces a sequence that goes through a transient series of digits before settling into a periodic sequence, then that generator is said to possess transients. The simplest example of such a generator is one which includes a register element outside any feedback loop which does feed or is fed by some element within a loop. As examples, consider the two generators of Figure 7. The first generator has a transient because of the delay stage at the end which is not connected in a loop. The second one has a transient because of stage 1, which feeds stage 2 but is not connected within a loop. Unless specified, the SRG's in this report have no transients.

Before concluding this section it should be pointed out that, as long as one restricts the feedback operations to addition and does not permit multiplication, the resulting generator will be a linear device and can



Initial Condition: 1001 Output: 1 0010111 0010111 - - - (Period 7)

or

Initial Condition: 1000 Output: 0 0010111 0010111 - - - (Period 7)

Figure 7. Two Examples of "Transient" Generators and Their Output Sequences

be expected to obey the usual laws of linear devices. For example, we shall see later that these shift-register generators obey the law of superposition.

## SECTION 2. FUNDAMENTAL PROPERTIES OF SRG SEQUENCES

When one connects a shift-register as a sequence generator, it is found that the output sequence is a function of the particular feedback connections made. Also, for some connections, the output sequence depends on the initial loading of the register. This has lead to the grouping of the output sequences into two types: maximal sequences and non-maximal sequences. This grouping is based on the "length" or "period" of the output sequence. For a given number of stages in a register there exists a maximum period for any output sequence; that is, there exists a maximum to the number of digits which occur before the sequence begins to repeat itself. It is quite easy to establish this number. Consider a simple generator of n stages; if, as it is shifted, the register successively contains every combination of n zero-and-ones then the output sequence will be the largest possible. Since there are $2^n$ different n-digit binary numbers, this would seem to be the maximum period possible. However, the sequence generator cannot possess all zeros in its stages (if it did, the generator would remain in this state and produce the all zero sequence); for this reason the largest possible period for a linear n stage shift-register is $2^n - 1$. Thus if a given output sequence has a period equal to $2^n - 1 = L$, then that sequence is called a maximal length sequence.

$$L = 2^n - 1 \qquad (1)$$

where L = length of maximal length sequence
n = number of stages in the shift-register generator

Example 1:Consider a generator of six stages, with feedback taps on 6 and 5. This generator is shown in Figure 3. With this connection a sequence 63 long is obtained; since $2^6 - 1 = 63$, this is a maximal sequence and contains all 6-tuples except the all zeros.

If a given output sequence has a period shorter than L, that sequence is termed a non-maximal length sequence. As stated in the introduction the traditional interest has been in maximal sequences; however, non-maximal ones may prove interesting in the future and this report deals with both types.

The feedback connections of a generator determine whether the output sequence will be maximal or non-maximal. Maximal sequences can be obtained from a generator with any number of stages (n). However, proper feedback connections must be chosen in order to produce a maximal sequence.

If with a given feedback connection one obtains a non-maximal sequence, then the output sequence depends also upon the initial load in the register. In other words, with a maximal length sequence one and only one sequence can be obtained from the connection; in the non-maximal case, however, a number of sequences can be obtained from that connection and which one of the possible is obtained depends upon the initial state of the register.

Among the various sequences obtained from the non-maximal connection one sequence is of more importance than the others: the "impulse response sequence." The impulse response sequence results when the register is loaded with all zeros except for either the first or the last stage. For an SSRG the output will then contain a one followed by n - 1 zeros and another one; this sequence is termed the impulse response. We shall later see the importance of this sequence in the non-maximal case; for the maximal sequence case, the single output sequence is the impulse response. Since the impulse response sequence (abbreviated IR sequence) is of special importance, we will label its length "$\ell$".

$$\ell = \text{Length of impulse response (IR) sequence.} \qquad (2)$$

Since $\ell$ is not uniquely related to the number of stages in the register we cannot write a relation such as equation (1) which applies to the maximal case.

Having introduced the concept of maximal and non-maximal sequences we are now in a position to formalize some basic properties of these two types of sequences. We shall state these basic theorems without proof; the proofs are given later in the Appendix.

Theorem 1: Given an n-stage shift-register generator, each n-tuple of binary digits appears once and only once among the sequences of this generator. Note that it may be necessary to place different initial loads in the register in order to see all n-tuples (the non-maximal case).

If all the n-tuples (except the all zero n-tuple) appear in the sequence before the sequence begins to repeat itself, then the generator is producing a maximal length sequence; and there are $2^n - 1$ total digits in a period of the sequence, as discussed earlier.

Corollary T1.1: If the sequence does repeat itself before all the n-tuples appear several non-maximal sequences occur, and one of these is the IR sequence. Further, the periods of the various sequences (omitting the all zero sequence) add the equal $2^n - 1$. Let $p_1$, $p_2$, $p_3$, etc., be the period lengths of the sequences other than the IR sequence. Then:

$$\ell + p_1 + p_2 + \ldots = 2^n - 1 = L \qquad (3)$$

where $\ell$ = period length of the impulse-response sequence;

$p$ = period length of other non-maximal sequences in the group.

In other words, given a generator which is connected to give non-maximal sequences, the sum of the periods of all the sequences add to equal the maximal length period.

Example 2: The eight stage generator with taps on 8 and 7 gives a set of non-maximal sequences. The IR response length ($\ell$) is 63; there are three more sequences of length 63 and one sequence of length 3. Hence the lengths add to $2^8 - 1 = 255$.

Theorem 2: The length of any sequence divides the length of the impulse-response sequence. The standard notation to indicate this is

$$p_i \mid \ell \qquad (4)$$

It should be kept in mind that it is not necessary for each $p_i$ to divide L, the maximal length period, since $\ell$ and L may be relatively prime. In the example of feedbacks on 8 and 7 above, it will be noted that the length of each sequence divides the IR length.

Another theorem which is important enough to consider at this point is the following:

Theorem 3: No simple shift-register generator which utilizes an odd number of feedback taps can produce a maximal length sequence.

The proof of this is seen as follows: consider filling the generator with all 1's; with an odd number of feedback taps the digit fed back will always be a 1 so that the resulting sequence will be all 1's with a period of one. Since the sum of the sequence periods must equal L, the longest sequence is at most L - 1; hence no odd number of feedbacks will produce a maximal sequence.

Therefore if we seek only those connections which result in maximal length sequences we need only consider those generators which utilize an even number of feedback taps.

A matter of importance at this point concerns the reverse of a given sequence. Given an SSRG with its output sequence, there exists a known related SSRG that will produce the reverse sequence of the original one. The reverse of a sequence " ... a b c ..." is the sequence " . . . c b a . . ."; that is, it is the sequence read in the reverse order. Every sequence of course has a reverse, but sometimes the reverse may be identical to the sequence itself; in this case the sequence (or SSRG connection) is called self-reverse. The procedure for finding the reverse SSRG is quite simple:
If an n-stage SSRG has feedback taps on stages n, k, m,...., the reverse generator will have feedback taps on stages n, n - k, n - m, ...., etc.

Example 3: Consider the generator of Figure 3, which has taps on stages 5 and 6. The reverse SSRG will have taps on stages 1 and 6. These are maximal generators, and the output sequence of the one is the reverse of the other. If a non-maximal SSRG is involved, each sequence from the reverse generator is the reverse of one of the sequences from the other.

Frequently it is of interest to determine the generator connections if one knows the output sequence. The following statement pertains to this: given an n-stage SSRG; if we know 2n - 1 digits of the output sequence of this generator we can uniquely determine the feedback connections.

The justification for the number 2n - 1 is that n digits are required as an initial condition, and n-1 additional digits are necessary to uniquely specify which of the taps are fed back. The $n^{th}$ stage feeds back, and one must determine if the first, the second, etc., to the $(n-1)^{st}$ stages are fed back. In general, one finds the feedback connections by using the standard methods of solving simultaneous equations. It is necessary to solve n-1 such equations, and it must be remembered that modulo-two arithmetic is involved. If the 2n - 1 digits of the sequence start with n-1 zeros followed by a one then a relatively short tabular method can be used to find the connections. This tabular method is outlined in figure 8 for a nine-stage generator.

. . . 0 0 0 0 0 0 0 0 1 1 1 1 1 0 1 1 1 0 0 1 1 0 . . .

Figure 8a) Part of the given sequence from a nine stage generator.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| 0 | | | | | | | | |
| 0 | | | | | | | | |
| 0 | | | | | | | | |
| 0 | | | | | | | | |
| 0 | | | | | | | | |
| 0 | | | | | | | | |
| 0 | | | | | | | | |
| 0 | | | | | | | | |

Figure 8b) Initial chart entries taken from the sequence as indicated.

| j<br>i | Y(0) | Y(1) | Y(2) | Y(3) | Y(4) | Y(5) | Y(6) | Y(7) | Y(8) |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| 2 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 3 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| 4 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 |
| 5 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| 6 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

Figure 8c) Chart completed by diagonalization of initial entries.
The column Y(j) is the contents of the register after j shifts.
The i-th row is the successive contents of the i-th stage.

$Y(0) \rightarrow Y(1)$: "1" IS in feedback
$Y(1) \rightarrow Y(2)$: "2" is NOT in feedback
$Y(2) \rightarrow Y(3)$: "3" is NOT in feedback
$Y(3) \rightarrow Y(4)$: "4" is NOT in feedback
$Y(4) \rightarrow Y(5)$: "5" IS in feedback
$Y(5) \rightarrow Y(6)$: "6" is NOT in feedback
$Y(6) \rightarrow Y(7)$: "7" IS in feedback
$Y(7) \rightarrow Y(8)$: "8" is NOT in feedback

Figure 8d) Steps used to determine that the feedback taps are 1, 5, and 7 in addition to 9.

Figure 8. Method for finding the simple generator from an impulse sequence

Part of the output sequence from a nine-stage generator is shown in Figure 8a; seventeen digits from this sequence are required to find the simple generator. The reader may use the remaining digits to check the result. The first two steps will form a chart of the nine successive register contents that are required in order to produce the given seventeen output digits. In the final step the shift of each successive content column into the next will be used to establish which of the stages, 1 through 8, are fed back in addition to the ninth.

The first step consists of writing the first seventeen digits of the sequence as shown in Figure 8b. Reading the sequence from left to right, one writes the first 9 digits vertically, starting at the bottom, and then continues the remaining 8 digits horizontally. The vertical digits are the initial content column and the horizontal row contains the digits which must appear successively in the first stage. It can be seen that this is the necessary arrangement of contents in order for the desired sequence to appear. The second step consists of filling in the content columns by repeating each initial entry on a descending diagonal, the exact duplicate of the manner in which the SSRG shifts its contents. The completed set of content columns is shown in Figure 8c.

In the final step one starts with the first content column (containing a single one in the first stage) and decides whether the first stage is fed back by considering the first digit of the second column. In the example it is apparent that stage one has a feedback tap in order to obtain a one in the first position of Y(1). Then, using Y(1), one considers whether stage 2 has a tap by comparing the contents of the first two positions of Y(1) with that of the first position of Y(2). In the example it is seen that stage 2 is not fed back; if the second stage did have a tap a zero would have been fed back to the first position of Y(2). Next one compares the first three contents of Y(2) with the first content of Y(3); Y(3) has no tap. This is continued until all stages have been treated. The success of this method lies with the fact that each stage j of contents has only zeros until the column Y(j-1); thus the content columns form a triangular matrix. Under this condition the associated equations can be solved one at a time by starting with the first and then moving downward, using the information from the previously solved equations. The complete logic for the example is given in Figure 8d. It should be remembered that the above method can be used as an alternative to solving equations simultaneously only if the given 2n-1 digits begin with n-1 zeros.

Another property of considerable importance in digital sequences is the "shift and add" property. This property is best introduced by considering two identical sequences being added together in a modulo-two fashion. If the resulting sum sequence is a shifted version of the original sequence, for any shift between the original two, then the original sequence is said to have the shift and add property. This property can be demonstrated with a single generator and a delay device, as in Figure 9. If the output sequence is a shifted version of the original for any amount of delay (quantized) then the sequence has the shift and add property.

It will be shown later that all maximal length sequences have the shift and add property. The non-maximal length sequences exhibit what may be termed a "partial" shift and add property; that is, particular shifts (delays) do result in obtaining the same sequence again but the remaining shifts do not.

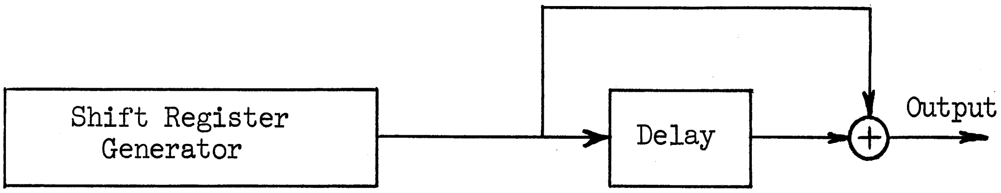


Figure 9. Illustrating the Shift and Add Property

The above properties, then, may be regarded as the most fundamental in the study of digital sequences. In the following section we begin the mathematical formulation for digital sequences. It is intended that the preceding material serve as a general picture to make the more detailed material which follows more easily understood.

## SECTION 3. MATHEMATICAL FORMULATION OF SHIFT REGISTERS AND SEQUENCES

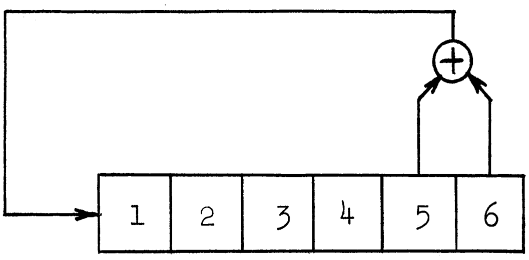
The chief object of this section will be to set up and explain the notation and mathematical formulation of SRG's and their sequences. These tools will then be applied to maximal sequences in Section 4 and to non-maximal sequences in Section 5.

### 3.1 The A Matrix

If we consider the contents of an n-stage shift register as an n-dimensional vector, it follows rather readily that the shift register is acting as a matrix operator on such vectors. Hence we should be able to represent any given shift register mathematically by a proper matrix. Also, since we are dealing with binary sequences, the field of the coefficients will be the integers 0 and 1 (mod 2).

We wish this matrix to perform the following function: given the n contents of an n stage generator, if we multiply the n column content vector by this matrix on the left, we obtain the contents of the generator after one shift. In other words, operating on the contents vector with the matrix performs the same function as running the generator a step at a time. In the literature (Ref. 4) this matrix has been called the "A" matrix, and this notation will be adopted in this report.

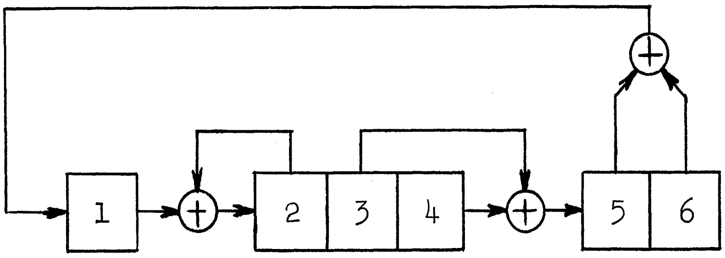
The A matrix is constructed in the following manner. First number the stages of the generator in the same direction as the contents travel under shifting. For n stages, the matrix will be n by n; identify each row of the matrix with the input to the corresponding stage in the register. In each row of the matrix we will place a 1 for each stage that feeds the stage corresponding to that row. Referring back to Figure 3 it is evident that, for a simple generator, we will always have a diagonal array of ones just below the diagonal since each stage is fed by its preceding stage except the first one. Let us construct the A matrix for the simple generator shown in Figure 3 and redrawn in Figure 10. Considering row 1, we note that stage 1 is fed by stages 5 and 6; hence in row 1 we place a 1 in the 5th and 6th columns. For row two, we see that stage 2 is fed by stage 1; for row 3, stage 3 is fed by stage 2, etc.. Hence the A matrix for this connection appears as shown in the Figure.



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

Figure 10. Constructing the A Matrix for the Generator Shown in Figure 3

Although most of the A matrices we will deal with will represent simple generators and hence be of the type shown in Figure 10, it is instructive to consider a more complex example. We take as a second example the multi-return generator shown in Figure 6.[1] Considering the rows corresponding to each stage, it will be seen that the A matrix is as shown in Figure 11.



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

Figure 11. Constructing the A Matrix for the Generator Shown in Figure 6

Suppose we load a generator with given initial conditions; then, if we consider this initial load as a n-row column vector, and multiply it by the A matrix on the left, we are doing the equivalent of shifting the generator by one step. The result is the contents of the generator after one shift. If we repeat this process, we find the contents of the generator after each shift. Therefore, multiplying on the left by a power of A is the same as shifting the register by that power. We can write this by using the matrix notation or by expressing the matrix operation as a summation. Equation 5 shows the function of the A matrix in both notations.

$$\begin{aligned} U(j + 1) &= A\,U(j) \\ u_i(j + 1) &= \sum_{k=1}^{n} a_{ik}u_k(j) \end{aligned} \qquad (5)$$

where: $u_i(j)$ = contents of the ith stage of the register after the jth shift.

$a_{ik}$ = elements of the A matrix.

[1] Using the impulse response of this generator and the reduction method of Figure 8, it is found that an SSRG with taps on 6, 4, and 1 produces the same sequences.

$$U(j) = \begin{bmatrix} u_1(j) \\ u_2(j) \\ u_3(j) \\ \vdots \\ u_n(j) \end{bmatrix} = \text{contents vector of register after } j \text{ shifts.}$$

From the preceding statements it follows that:

$$\begin{aligned} U(j+2) &= A^2\,U(j) \\ U(j+3) &= A^3\,U(j) \\ &\;\;\vdots \\ U(j+m) &= A^m\,U(j) \end{aligned} \qquad (6)$$

The order of a matrix is given by that lowest power of the matrix which yields the identity matrix. From equation (6) it is seen that when $A^m = I$, both vectors in the equation are the same. Hence the period of the sequence from a generator will be given by the order of the matrix which represents that generator. This means, in the maximal length case, that

$$A^L = A^{2^n - 1} = I \qquad (7)$$

For the non-maximal length case it means that:

$$A^{\ell} = I \qquad (8)$$

Equation (8) is not obvious from the above reasoning, and is proved in Appendix A.2. The proof rests on Theorem 2, which states that "the period of any sequence from an SSRG divides the IR sequence period." It should be emphasized that the importance of the IR sequence, mentioned before, stems from Theorem 2 and Equation (8).

It should be noted that in the non-maximal case there will be sequences with periods shorter than $\ell$ but since, by Theorem 2, the length of every sequence divides the IR period, these shorter sequences will also be periodic every $\ell$ digits.

The inverse of the A matrix plays the role of running the generator backwards. It can easily be shown (Appendix A.1) that every simple generator has a matrix which is non-singular and hence has an inverse; a consequence of this is that it will have no transients. Also, any multiple-return generator's matrix has an inverse unless the generator is so constructed as to have transients.

### 3.2 The Characteristic Equation

Having established the construction and meaning of the A matrix, we now wish to consider the "characteristic equation" of the A matrix. In general, when dealing with matrices, the characteristic equation is of great value for mathematical manipulations. In the cases here we shall find this equation of great value in determining the structure behind digital sequences.

In general the characteristic equation of any n x n matrix (A) is an nth degree equation formed by setting the determinant $|A - \xi I|$ equal to zero. Since the coefficients are taken from the field of integers modulo-two it makes no difference whether we consider the minus sign to be a plus sign. In addition, the "characteristic polynomial" is the determinant itself (without setting it equal to zero.)

Characteristic Polynominal of A: $|A - \xi I|$ (9)

Characteristic Equation of A: $|A - \xi I| \equiv 0 \pmod 2$

Although one can always find the characteristic equation by considering the determinant, it is simpler in some cases to use the companion matrix for this purpose.[1] With every equation there is associated a "companion matrix," and the matrix is defined as follows: If the equation is

$$\xi^n + c_1 \xi^{n-1} + c_2\xi^{n-2} + \dots\dots + c_n \equiv 0 \pmod 2 \qquad (10)$$

then the companion matrix is

[1] The companion matrix refers to either the form as in equation (11) or its transpose. (Ref. 5) uses one form and (Ref. 6) uses the other.

$$\text{companion matrix} = \begin{bmatrix} 0\,1\,0\,0\,0 \ldots\ldots 0 \\ 0\,0\,1\,0\,0 \ldots\ldots 0 \\ 0\,0\,0\,1\,0 \ldots\ldots 0 \\ 0\,0\,0\,0\,1 \ldots\ldots 0 \\ \vdots \qquad\qquad\qquad \vdots \\ c_n\; c_{n-1} \cdots\cdots c_1 \end{bmatrix} \tag{11}$$

It must be emphasized that the plus signs in equation (10) signify modulo-2 addition. In fact, for the remainder of this report, any equation whose unknowns are matrices will involve modulo-2 addition.

The object now is to note that, if one is given a companion matrix, then one can read off the characteristic equation by looking at the last row. The companion matrix will also play a part in considering the equivalent SSRG of multiple-return generators which have no transients.

Referring to the generator matrix of Figure 10, we note that this matrix is only a rotation away from being a companion matrix.[2] This will be true for all SSRG's and can be stated as follows: the A matrix resulting from any SSRG is only a rotation away from being a companion matrix. Therefore to find the characteristic equation of a simple generator we need only take the A matrix, rotate it and then use equation(11). Since the first row of the A matrix for a SSRG is directly related to the feedback taps, a direct relation exists between the taps and the characteristic equation. This relation can be stated formally: if the feedback taps are on stages n, k, m, etc., the characteristic equation will be:

$$\xi^{n} + \xi^{n-k} + \xi^{n-m} + \ldots.+I \equiv 0, \ (\text{mod } 2) \tag{12}$$

where n, k, m. etc. = stages fed back in simple generator.

Observe that a feedback tap will always occur in the nth stage; if this were not true we would merely be shortening the register, and its length would no longer be n.

[2] $A^R$ is the "rotate" of A if $a^R{}_{ij} = a_{n-i+1,\ n-j+1}$

If we write an equation where the powers appearing are the stages fed back in one generator we have the characteristic equation for the reverse generator. In other words, if we have feedback taps on stages n, k, and m, and write an equation:

$$\xi^n + \xi^k + \xi^m + I \equiv 0, \pmod 2 \qquad (13)$$

this is the characteristic equation of the generator that produces the reverse sequence from that produced by matrix A.

Now, by the Caley-Hamilton Theorem (Ref.5), the matrix satisfies its own characteristic equation; therefore the important matrix equation corresponding to a SSRG with feedback taps on n, k, m, etc. is:

$$A^n + A^{n-k} + A^{n-m} + \ldots\ldots I \equiv 0 \pmod 2 \quad (14)$$

Example 4: Consider the SSRG of Figure 10. Since there are feedback taps on stages 5 and 6, the use of equation (14) specifies that the characteristic equation is:

$$A^6 + A + I \equiv 0 \qquad (14a)$$

In this manner, then, the characteristic equation can be determined for any SSRG.

In view of the relation between feedback taps and characteristic equations for SSRG's, we wish to set up a notation convention that will be used throughout this report. The convention is as follows:

[n, k, m, ... 0]: feedback equation and specifies feedback taps of a simple generator on stages n, k, m, ... . (15)

(n, k, m, ... 0): polynominal, $\xi^n + \xi^k + \xi^m + \ldots + 1$.

Note that a 0 has been rather fictitiously placed in the feedback equation (there is no feedback tap from a zero stage), but the value of this will appear later.

As two examples of this convention, consider the following:[1]

$A_1 \leftrightarrow [6,5,0] \Longleftrightarrow (6,1,0)$ is the characteristic polynomal of $A_1 \Longrightarrow$

$$A_1^6 + A_1 + I \equiv 0 \qquad (16)$$

$A_2 \leftrightarrow [8,7,4,3,0] \Longleftrightarrow (8,5,4,1,0)$ is the characteristic polynominal of $A_2 \Longrightarrow$

$$A_2^8 + A_2^5 + A_2^4 + A_2 + I \equiv 0$$

In the first example there are feedback taps on stages 6 and 5; in the second case the taps are on stages 8,7,4, and 3. The purpose of this simplified notation is merely to avoid the labor of writing the symbol A again and again.

It is of interest to note the reverse of each of the examples of equation (16). The reverses are, respectively:

$$[6,1,0] \Longleftrightarrow (6,5,0) \Longrightarrow A^6 + A^5 + I \equiv 0$$

$$[8,5,4,1,0] \Longleftrightarrow (8,7,4,3,0) \Longrightarrow A^8 + A^7 + A^4 + A^3 + I \equiv 0 \qquad (17)$$

The relation between feedback equations, characteristic equations and the reverse equations illustrated by equations (16) and (17) should be studied carefully to avoid confusion.

To find the characteristic equation of a multiple-return generator, the determinant of equation (9) must be evaluated. For the multiple-return case the constant term ($c_n$) of the characteristic equation plays an important part. If the equation has a non-zero constant term, then the companion matrix of this equation will be the rotate of the A matrix for some SSRG. This SSRG will then be the "equivalent SSRG" for the given multiple-return generator. By "equivalent" we mean that all the sequences from the one generator can be obtained from the SSRG. In section A.2 of the Appendix this equivalence is proved, and it is shown that such multiple-return generators will have no transients.

[1] The single arrow ↔ denotes correspondence, while the double arrows are implications. ⟹ is read "implies" while the double implication ⟺ is read "if and only if".

On the other hand, if the characteristic equation of a multiple-return generator has a zero constant term there will be no equivalent SSRG. Such a generator will produce short transients, and there exists an SSRG of fewer stages which will produce the periodic sections of the sequences. In fact, the sequences---transient and periodic part together---can be produced by an n-stage SRG in which all of the feedbacks are to a single stage. This will not be an SSRG, however, since for this a feedback would appear from the last stage and all taps would be connected to the first stage.

Even for these transient generators, however, we would be most interested in the periodic portion because, for an n-stage generator, the transient is at most n-digits long, while the period may be $2^n - 1$ digits long. For a 20 stage generator, for example, the longest transient is twenty digits long compared to a maximum period of over a million digits. For the remainder of this report, then, we shall be concerned specifically with SSRG's or those multiple-return generators which have simple equivalents (unless mentioned otherwise).

The importance of the material on the preceding pages lies in the fact that, by considering the characteristic equations of generators as general polynomials we can apply the tools of algebra to find the structure behind digital sequences. It is of major importance to determine whether the polynomials are reducible or irreducible; and if reducible, what their factors are. Table II on pages 41 and 42 lists all the polynomials resulting from simple generators with an even number of feedback taps through the 8th degree. The factors of those polynomials that are reducible are also shown.

In the following two sections these polynomials and their factors (if any) will be used to portray the structure of maximal and non-maximal sequences. The purpose of this section is to set up and explain the notation and the mathematical formulation; the application of these tools to the sequences themselves are given in Sections 4 and 5.

### 3.3 The Feedback and the Sequence Laws

Thus far we have considered the construction and meaning of the A matrix, and the treatment of the characteristic equations of the A matrices as polynomials which may or may not be factorable. It was noted that the A matrix stems from the generator itself, and that the simple generator is the most important; every multiple-return generator (that contains no transients) has an equivalent simple generator. We now wish to consider two laws that apply to the sequences that are produced by the generators. The two laws referred to we have chosen to call the "feedback law" and the "characteristic sequence law." These two laws are very closely related to the characteristic equation and even more closely related to each other. As a matter of fact, the sequence law and the feedback law are simply two slightly different ways of looking at the same thing.

Consider a digital sequence that has been generated by a shift-generator. As time proceeds and we step the generator with regularly spaced shift pulses, we can regard the generation of the sequence in two different ways. In the first place we can envisage a simple generator being placed above the sequence (the stages aligned with the digits), and consider the register to move to the right, one step at a time, as the generator is run. This is depicted in Figure 12. If the generator stages are numbered in the usual way and the output is considered as being taken from the first stage, then the register above the sequence must be numbered from right to left as shown in the Figure. A little thought will convince one that, as the actual generator is run, moving the fictitious register above the sequence to the right will correctly display the contents of the generator at each time, and correctly show the generation of the sequence. From this simple illustration we immediately verify the "feedback law". This refers to the fact that, given an initial loading of the generator, we can construct the rest of the sequence by noting the feedback taps on the register, forming the modulo-two sum of the contents of the feedback stages, and placing the result in the 0th stage (the stage to the right of stage 1). This is indicated by the arrows beneath the sequence in Figure 13. A practical way to form a sequence on paper is to assume an initial load, make a template of arrows such as is shown, and then slide this template to the right. The feedback law is merely the generalization of this phenomenon and is now stated:

Feedback law: Given a feedback equation and the initial contents of a simple generator, the entire sequence can be generated by successive applications of the feedback equation. Suppose the feedback equation is [n,k,m,0], which implies feedback taps on the $n^{th}$, $k^{th}$, and $m^{th}$ stages, then the feedback law is:

$$u_n(j) + u_k(j) + u_m(j) \equiv u_0(j) \pmod 2 \qquad (18)$$

where $u_n(j)$ = contents of the $n^{th}$ stage after j shifts.

This is the mathematical equivalent of moving the template of arrows to the right, as was done in Figure 13. Note that the time shifts (j) play no important part in this equation; if the time reference is arbitrary the j's should be omitted.

The second way to view the generation of the sequence is to consider, not the entire register, but only one stage (preferably the last), and relate the past contents of that stage with the future contents. Viewing the generation in this manner results in what we term the "characteristic sequence law."

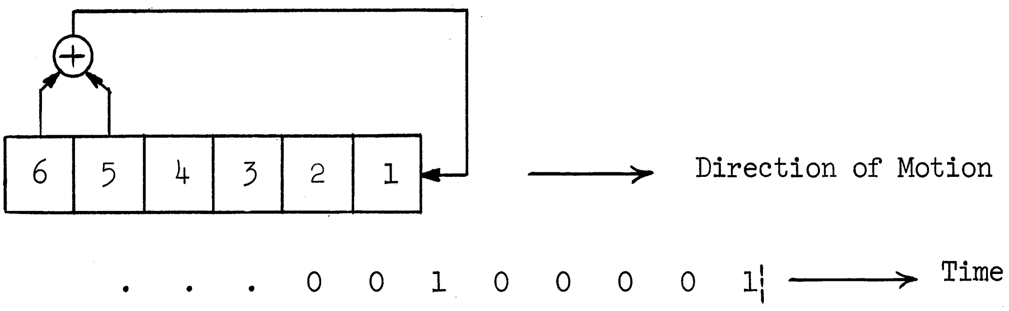


Figure 12: Sequence and Register [6,5,0]

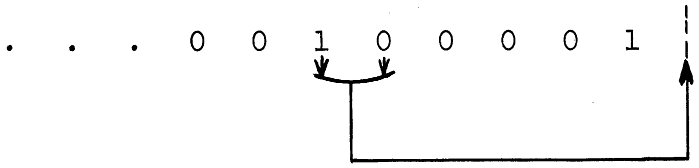


Figure 13: Generation of Sequence by Considering Feedback Law

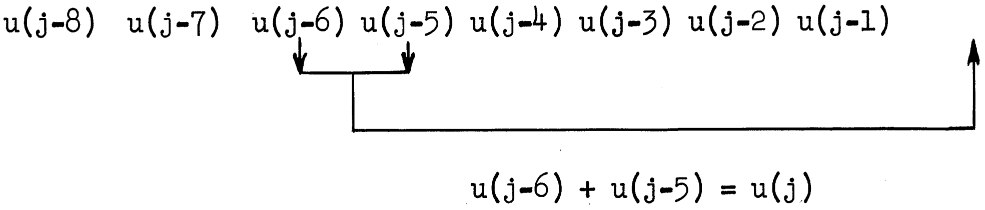


Figure 14: Generation of Sequence by Considering Sequence Law.

Characteristic Sequence Law: The content of each stage of a simple shift register generator satisfies the feedback equation. If the given feedback equation is [n,k,m,0] then the corresponding sequence law is:

$$u_i(j-n) + u_i(j-k) + u_i(j-m) \equiv u_i(j) \pmod 2 \qquad (19)$$

where $u_i(j)$ = contents of $i^{th}$ stage after j shifts.

This equation says that the present contents of stage i is formed from the modulo-two sum of the contents of the $i^{th}$ stage after -n shifts, -k shifts, and -m shifts; of course negative shifts correspond to previous contents. Considering the fact that, with a simple generator, the contents of the $j^{th}$ stage after -k shifts is equal to the present content of the (j + k) stage, the sequence law is easily justifiable; a mathematical proof is contained in the appendix. Figure 14 shows the concept of this sequence law. Note that a given sequence will obey a number of laws, but this particular characteristic law is directly related to the method of generation. An immediate consequence is that all sequences from a given generator obey the characteristic sequence law.

Although the feedback law and the above sequence law deal with the same thing, it is noted that the feedback law of equation (18) contains stage numbers as the variable, and for the sequence law time shifts is the variable. For this reason the distinction between the two laws should be kept in mind. Equation (20) gives the conversion which allows a feedback law to be changed to a sequence law for a simple SRG, and vice versa.

$$u_i(j-k) = u_k(j-i) \qquad 0 \leq i,\ k \leq n \qquad (20)$$

which is a special case of:

$$u_j(k) = u_{j+a}\ (k+a) \qquad -j \leq a \leq n-j \qquad (20a)$$

To recapitulate, the feedback law and the sequence law are additional tools for studying digital sequences. They are useful for constructing sequences, knowing the initial loading, and are useful for studying other structure properties of digital sequences.

## 3.4 The $B_A$ Matrix

The remaining tools which we have to consider in this section consist of two additional matrices. Both of these play a role in studying the structure of digital sequences.

The first of these is called the $B_A$ matrix (Ref. 4), and it is a useful tool both for finding the proper connections for maximal generators and for illustrating the superposition property of shift-register generators. The notation "$B_A$" is used to emphasize the fact that any $B_A$ matrix is uniquely associated with a specific A matrix. We remember that the A matrix is construed as that matrix which operates on the content vector of the simple generator to produce the content vector after one shift. Also, that the various powers of the A matrix correspond to the respective shifts. We shall find it necessary, later, to be able to express all the powers of the A matrix in terms of powers of A which are no larger than n-1 (n is the number of stages). In other words, we wish to find coefficients such that, for every k, we can form the relation:

$$A^k = \sum_{i=1}^{n} b_{ki} A^{n-i} \qquad (21)$$

Note that the variable i ranges only from 1 to n:

If we desire to know this relation for all k ($k \leq L$ for the maximal length case and $k \leq \ell$ for the non-maximal case), the coefficients $b_{ki}$ will form either an L by n or an $\ell$ by n matrix. It is this matrix which we shall call the $B_A$ matrix.

The construction of the $B_A$ matrix consists essentially of successively raising the powers in an equation, starting with the identity A = A, and ending with $A^{\ell} = I$. Whenever the power n appears on the right hand side, it is replaced by use of the characteristic equation. Of course, the first n-l equations will consist merely of setting the term equal to itself; consequently the first n-l terms form an off-diagonal array.

Example 5: As an example we will construct the $B_A$ matrix for the generator [4,2,0]. The A matrix and its companion matrix are shown in Figure 15. This generator is self reverse, and the characteristic equation in this case is (4,2,0).

$$A = \begin{bmatrix} 0&1&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \end{bmatrix} \qquad \text{Companion of } A = \begin{bmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&0&1&0 \end{bmatrix}$$

Figure 15. The A and Its Companion Matrix for the Generator [4,2,0]

Solving for the $n^{th}$ degree term in the characteristic equation, ($A^4 = A^2 + I$) and using this relation as the powers are successively raised, the following equations are found:

$$\begin{aligned} A &\equiv A \\ A^2 &\equiv A^2 \\ A^3 &\equiv A^3 \\ A^4 &\equiv A^2 + I \qquad\qquad (\text{mod } 2) \qquad\qquad (22) \\ A^5 &\equiv A^3 + A \\ A^6 &\equiv A^4 + A^2 \equiv I \end{aligned}$$

From this we see that $A^6 = I$, and hence the impulse response length of this generator is 6. From these equations the following $B_A$ matrix is formed; although the matrix is here written somewhat as a table, we shall refer to the quantities inside as the $B_A$ matrix.

| Power of A | 3 | 2 | 1 | 0 |
|---|---|---|---|---|
| 1 | 0 | 0 | 1 | 0 |
| 2 | 0 | 1 | 0 | 0 |
| 3 | 1 | 0 | 0 | 0 |
| 4 | 0 | 1 | 0 | 1 |
| 5 | 1 | 0 | 1 | 0 |
| 6 | 0 | 0 | 0 | 1 |

(23)

In the above manner then the $B_A$ matrix is constructed from the A matrix.

Referring now to equation (21) and to equation (6), it immediately follows that:

$$Y(k) = \sum_{i=1}^{n} b_{ki}\ Y(n-i) = \sum_{j=o}^{n-1} b_{k,n-j}Y(j) \qquad (\text{mod } 2) \qquad (24)$$

This equation relates the content vector after k shifts to the content vector after j shifts, where j ranges from 0 to n-1. Thus the $B_A$ matrix is seen to relate the content vector for any k shifts (i.e., for n digits anywhere in the sequence) to the content vectors of the first n-1 shifts.

Also, using the $B_A$ matrix we can quickly verify all sequence laws; we need only write the equation corresponding to any one stage of the content vectors of equations (24):

$$u(k) \equiv \sum_{i=1}^{n} b_{ki}u(n-i) \equiv \sum_{j=o}^{n-1} b_{k,n-j}u(j) \quad (\text{mod } 2) \qquad (25)$$

For our purposes the most important use of the $B_A$ matrix will be to find the proper connections to produce maximal sequences. This will be treated in Section 4. Another interesting use, however, lies in the following: if we read the $j^{th}$ column of the $B_A$ matrix, we obtain the sequence which results from a simple generator with a single one in the $j^{th}$ position. Hence this is one way of determining the impulse response sequence for a simple generator (the first or the last column). If the generator produces a maximal length sequence, then only one will appear. If, however, the generator is a non-maximal one, then the various sequences which can be produced may be obtained by adding (modulo-two) the various columns of the $B_A$ matrix, two at a time, three at a time, etc. When all the n-tuples have occurred in the resulting sequences, then all the possible sequences will have been obtained. Since each individual column represents the response to an elementary load, this addition of the columns to obtain the non-maximal length sequences amounts to a superposition of elementary responses. This is possible because the generators we have been considering are linear devices which in turn is due to the arithmetic operations being limited to addition. We shall consider an application of this in Section 5.

### 3.5 The C Matrix

The remaining matrix to be introduced in this section is called the commutating (C) matrix, and its use is in giving the relation between non-maximal sequences of a generator. It has been found that when the characteristic polynomial is irreducible, but the output is not maximal length, a number of non-maximal length sequences of the same length will appear. Further, it has been found that there exists a matrix which permutes among these equal-length sequences. Any such matrix has been termed the C matrix. As a further result it has been determined that if a generator is wired corresponding to this C matrix, the permuted sequences can all be obtained by a time sampling of the resulting sequence. At this point the significance of these results lie in that they indicate additional structure which may well be important in later work. The C matrix and its implications will be considered in detail in Section 5.

## SECTION 4. MAXIMAL LENGTH SEQUENCES

In the preceding section we have introduced a notation and general mathematical formulation for studying digital sequences. In this section we wish to use these tools to study in a rather detailed manner maximal length sequences and the generators which furnish them. We will deal with such questions as: How many maximal length sequences are available from an n stage generator? What connections of the n stage generator provide these maximal sequences? Do multiple-return generators give sequences not available for simple generators? What shift and add properties do maximal length sequences have? and What are the important statistical properties of maximal length sequences?

## 4.1 Determining the Number of Maximal Sequences

Given an n stage shift register generator, it was noted in Section 2 that certain feedback connections will give maximal length sequences, and the other connections will produce a set of shorter sequences (non-maximal length). A sequence is said to be maximally long if its period is related to the number of stages (n), and if the period is $2^n - 1$. It was noted in the introduction that thus far in the applications of digital sequences, the maximal length ones have been of greatest interest.

We first consider how many maximally long sequences are available from a given n stage generator. Zierler (Ref. 4) has shown the following result, which we state as a theorem:

Theorem 4: For an n stage register there are exactly $\frac{\phi(2^n - 1)}{n}$ sequences of maximal length available with proper feedback connections. Here $\phi(2^n - 1)$ is Euler's phi function and is defined as follows: $\phi(k)$ is the number of positive integers less than k and relatively prime to k, including 1; i.e., $\phi(k)$ is the number of integers less than k that have no common factor with k.

Example 6: Consider a 5 stage generator. $2^5 - 1 = 31$; hence we seek the value of $\phi(31)$. Since every integer less than 31 is relatively prime to 31, there are 30 integers less than 31 and prime to 31; hence $\phi(31) = 30$. Dividing this by 5, the number of stages, the result states that there are 6 maximally long sequences possible with a 5 stage shift register generator.

Zierler's proof is stated as follows: In order for an SRG to produce a maximal length sequence, the characteristic equation of the generator must be the minimum polynomial of a primitive $L^{th}$ root of unity. Further, there are exactly $\frac{\phi(2^n - 1)}{n}$ different equations of degree n that are minimum equations of primitive $L^{th}$ roots of unity. For this reason the above theorem is true.

The fact that the number of maximal sequences available is $\frac{\phi(2^n - 1)}{n}$ can be justified by the following reasoning. Suppose that we take any one of the maximal length sequences from an n stage generator. Further, suppose we time sample the digits from this sequence; i.e., take every second digit, take every third digit, etc. Now if we time sample with rates that are relatively prime to the length L, then we will not get any sub-periods and every sequence obtained will also be maximal. It is obvious that if we sample at a rate that is a factor of L, a sub-period will be obtained, and the resulting sequence will not be maximal. Using only these relatively prime rates, then, all the maximal sequences will be obtained, and the number of sequences obtained will be $\phi(2^n - 1)$. But Zierler's rule states that all of these sequences (which could be obtained by time sampling a maximal sequence at prime rates) fall into sets of n, so that there are n of each kind and hence there would be $\frac{\phi(2^n - 1)}{n}$ different maximal sequences.

To justify this grouping into sets of n we need to consider the characteristic equation for the originally chosen sequence. Given that the A matrix for the original sequence satisfies the characteristic equation, then $A^2$ also satisfies this equation; and the square of $A^2$ $(A^4)$, etc. This is true because squaring a polynomial that involves modulo-two addition amounts to merely doubling each exponent in the equation.[1] Consider the equation $A^6 + A^5 + I = 0$. Squaring this equation, it is found that $A^2$ also

[1] In general, the product of two polynomials, modulo-two, is equal to the ordinary product of the two polynomials with the resulting coefficients reduced mod-2.

satisfies the same equation:

$$
\begin{aligned}
(A^6 + A^5 + I)^2 &= A^{12} + 2A^{11} + A^{10} + 2A^6 + 2A^5 + I \\
&\equiv A^{12} + A^{10} + I \qquad (\text{mod } 2) \qquad\qquad (26)\\
&= (A^2)^6 + (A^2)^5 + I
\end{aligned}
$$

$$(A^6 + A^5 + I \equiv 0 \quad (\text{mod } 2) \implies (A^2)^6 + (A^2)^5 + I \equiv 0 \ (\text{mod } 2)$$

Hence A, $A^2$, $A^4$, $A^8$, etc., all satisfy all of the same equations; hence the resulting sequences will all obey the same characteristic sequence law. This, of course, means that the generators corresponding to A, $A^2$, $A^4$, etc., all generate the same sequences. It remains to note that using a generator of matrix $A^2$ is the same as time sampling every second digit of the sequence from the generator whose matrix is A; similarly, $A^4$ is the same as sampling every 4th digit of the sequence, etc. Therefore, in the entire set of sequences obtained above by sampling, all those whose matrices are related by squares form the same sequence and this is the basis for grouping the entire set of sequences. In effect then, we take every power relatively prime to $2^n - 1$ and group all those powers that are related by factors of two; in this process one must proceed past the power $2^n - 1$ and then subtract $2^n - 1$ in order to get all the proper powers. Since $2 \cdot [2^{n-1}p] \equiv p \ (\text{mod } 2^n - 1)$ there are n numbers to each set formed in this manner, and the set of resulting matrices is called a "similarity class." The following example should clarify this process:

Example 7: Consider a 5 stage generator; the feedback equation [5,3,0] will give a maximal length sequence. Earlier we learned that there are 6 maximal sequences, and that Ø(31) equals 30. Hence by time sampling any one maximal sequence (the one from [5,3,0] for example) at the relatively prime rates (1 through 30) 30 maximal sequences will result. To show these fall into sets with 5 in each set, we group all the powers which are related by doubling.

$$\begin{array}{ll} 1. & A, A^2, A^4, A^8, A^{16} \\ 2. & A^3, A^6, A^{12}, A^{24}, A^{17} \\ 3. & A^5, A^{10}, A^{20}, A^9, A^{18} \\ 4. & A^7, A^{14}, A^{28}, A^{25}, A^{19} \\ 5. & A^{11}, A^{22}, A^{13}, A^{26}, A^{21} \\ 6. & A^{15}, A^{30}, A^{29}, A^{27}, A^{23} \end{array} \tag{27}$$

In this way all the sequences acquired from time sampling one maximal sequence fall into 6 sets, and there are $\frac{\phi(2^5-1)}{5}$ such classes.

This then is a qualitative justification for the number of maximal sequences being equal to $\frac{\phi(2^n - 1)}{n}$.

The calculation of the number $\phi(k)$ falls into two cases on depending upon whether k contains factors or is prime. If k is factorable, then the following relation exists for calculating $\phi(k)$:

$$\phi(k) = k \prod \frac{(p_i-1)}{p_i} \tag{28}$$

where $p_i$ are the prime factors of k.

Example 8: Consider a 6 stage generator where it is necessary to know $\phi(63)$. The prime factors of 63 are 3 and 7; hence the equation yields

$$\phi(63) = 63 \times \frac{(2)(6)}{(3)(7)} = 36 \tag{29}$$

When k is a prime number,

$$\phi(k) = k-1 \tag{30}$$

With the use of equations (28) and (30) the number of maximal length sequences available from a generator of a given number of stages can be determined.

Table 1 shows the number of maximal sequences for generators up to length 21. In this table the number $2^n - 1$, the number of maximal length sequences, and the factors of $2^n - 1$ are shown. Figure 16 shows the values as points on a graph. In this figure an upper bound curve is also drawn.

## Table 1

| Number of Stages | Maximal Seq. Length | Number of Max. Length | Factors of $2^n$-1 |
|---|---|---|---|
| n | $2^n$-1 | $\frac{\phi(2^n-1)}{n}$ | |
| 2 | 3 | 1 | |
| 3 | 7 | 2 | |
| 4 | 15 | 2 | $3\cdot5$ |
| 5 | 31 | 6 | |
| 6 | 63 | 6 | $3^2\cdot7$ |
| 7 | 127 | 18 | $3\cdot5\cdot17$ |
| 8 | 255 | 16 | $3\cdot5\cdot17$ |
| 9 | 511 | 42 | $7\cdot73$ |
| 10 | 1023 | 60 | $3\cdot11\cdot31$ |
| 11 | 2047 | 176 | $23\cdot89$ |
| 12 | 4095 | 144 | $3^2\cdot5\cdot7\cdot13$ |
| 13 | 8191 | 630 | |
| 14 | 16383 | 756 | $3\cdot43\cdot127$ |
| 15 | 32767 | 1800 | $7\cdot31\cdot151$ |
| 16 | 65535 | 1536 | $3\cdot5\cdot17\cdot257$ |
| 17 | 131071 | 7710 | |
| 18 | 262143 | 7776 | $3^2\cdot7\cdot19\cdot73$ |
| 19 | 524287 | 27594 | |
| 20 | 1048575 | 24000 | $3\cdot5^2\cdot11\cdot31\cdot41$ |
| 21 | 2097151 | 84672 | $7^2\cdot127\cdot337$ |

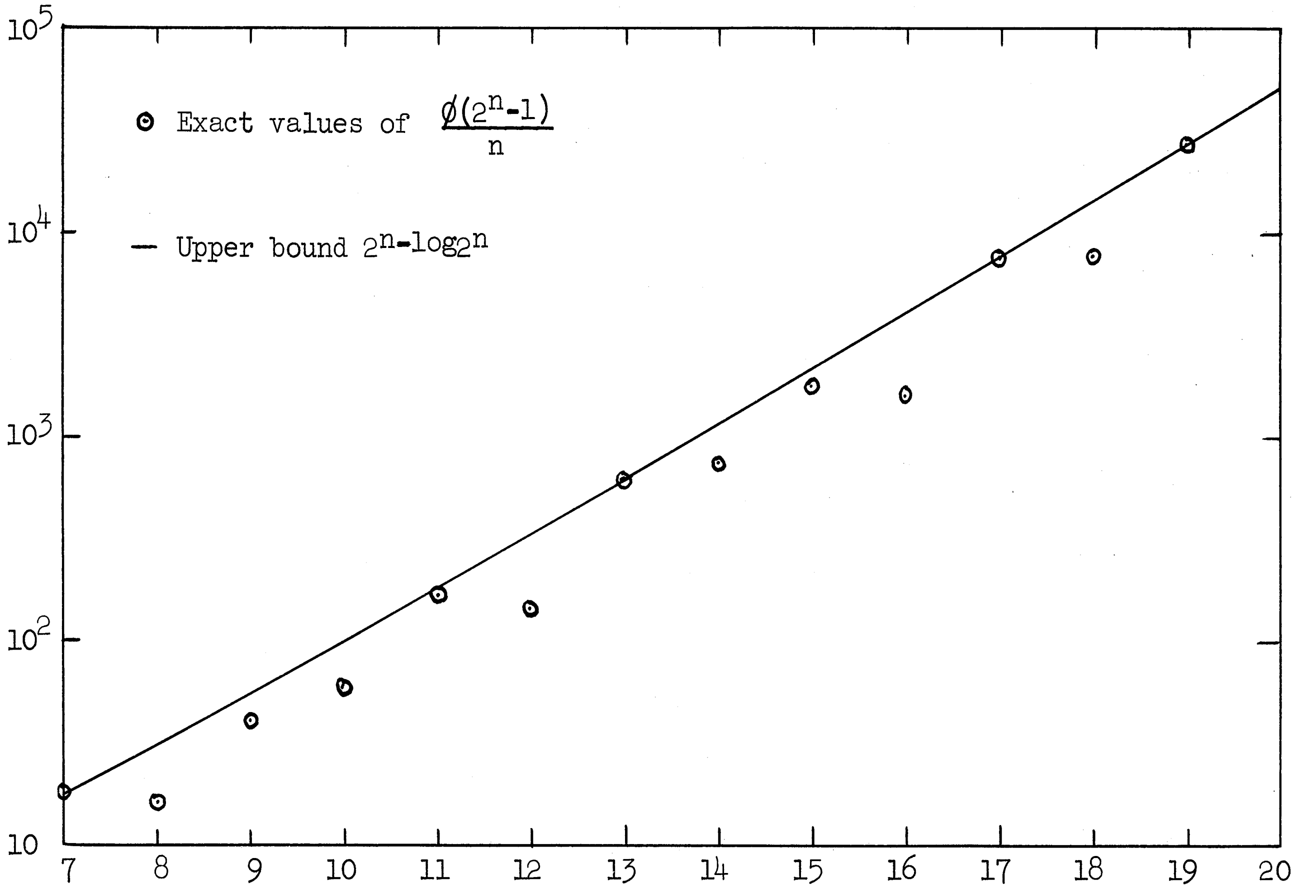


Figure 16. Comparison of the number of maximal sequences with the bound

The equation for the upper bound is

$$\frac{\phi(2^n-1)}{n} < 2^{n-\log_2 n} \qquad (31)$$

Given the number of sequences desired, the upper bound curve can be used to specify approximately the necessary number of stages; an n of this order will always be satisfactory.

## 4.2 Determining the Connections for Maximal Sequences

The question of how many maximal sequences are available from a given number of stages has now been dealt with. The next question that appears deals with what connections provide these maximal sequences. This query is of no mean importance; for example with an 8 stage generator there are 16 maximal length sequences available, but there are 128 different possible ways of connecting the register as a simple SRG. The major tool for dealing with the question of proper connections will be the polynomials which represent the characteristic equations of the possible connections; cognizance of the material in Section 3 will be assumed in this section.

First, we wish to recall Theorem 3 which appeared in Section 2. This theorem states that no generator which utilizes an odd number of feedback taps can produce maximal length sequences. Hence this eliminates approximately one-half of the possible connections from our consideration. Relating this to polynomials, this means that when the identity term is included (the 0 term in the notation), the polynomial will have an odd number of terms. In the future, then, we will consider only those generators which have an even number of feedback taps or those polynomials which have an odd number of terms.

Two methods for finding those connections which provide maximally long sequences will be described in the following pages. Although the second method (developed later than the first) is preferable to the first, there is sufficient pertinent material in the first to prevent discarding it.

### 4.2.1 First method

The first method, to be described in the ensuing material, is based on the following theorem:

Theorem 5: No generator whose characteristic equation is a reducible polynomial can generate maximal sequences.

The proof lies in the fact that, for a maximal sequence, the characteristic equation must be a minimum polynomial of a primitive $L^{th}$ root of unity (stated earlier). Obviously, if a polynomial is factorable it is not a minimum polynomial.

Note that this theorem does not say that every polynomial that is irreducible represents a maximal sequence generator; this theorem simply eliminates a large class of possible connections. Considering the list of irreducible polynomials, there still remains some elimination to find those connections which do produce maximal sequences.

To make a listing of the connections which provide maximal sequences, then, one could make a list of all the polynomials (a generator of n stages corresponds to a polynomial of $n^{th}$ degree) with an odd number of terms. Then one would investigate each of these to find those that are irreducible. Table II shows a list of all such polynomials and their factors, if any, from degree 2 through 8; hence these correspond to generators up to eight stages long. Observe that the notation introduced in Section 3, equation (15) is used, and also that those connections which provide sequences that are the reverse of each other are paired (shown in the same row). In this respect, also note that the factors of a reverse polynomial are the reverse of the other polynomial's factors.

The entries shown in this table were obtained by brute force; in order to find the factorable polynomials of $n^{th}$ degree, all lesser degree polynomials which multiply to form an $n^{th}$ degree polynomial were multiplied.

Table II

| Length, $\ell$ | Polynomial | Factors of Polynomial | Reverse of Polynomial |
|---|---|---|---|
| L = 3 | (2,1,0) | | (2,1,0) |
| L = 7 | (3,1,0) | | (3,2,0) |
| L = 15 | (4,1,0) | | (4,3,0) |
| $\ell$ = 6 | (4,2,0) | $(2,1,0)^2$ | (4,2,0) |
| $\ell$ = 5 | (4,3,2,1,0) | | (4,3,2,1,0) |
| $\ell$ = 21 | (5,4,0) | (2,1,0)(3,1,0) | (5,1,0) |
| L = 31 | (5,2,0) | | (5,3,0) |
| L = 31 | (5,3,2,1,0) | | (5,4,3,2,0) |
| L = 31 | (5,4,2,1,0) | | (5,4,3,1,0) |
| L = 63 | (6,1,0) | | (6,5,0) |
| $\ell$ = 14 | (6,2,0) | $(3,1,0)^2$ | (6,4,0) |
| $\ell$ = 9 | (6,3,0) | | (6,3,0) |
| $\ell$ = 15 | (6,5,4,3,0) | (2,1,0)(4,1,0) | (6,3,2,1,0) |
| $\ell$ = 21 | (6,4,2,1,0) | | (6,5,4,2,0) |
| L = 63 | (6,5,2,1,0) | | (6,5,4,1,0) |
| L = 63 | (6,4,3,1,0) | | (6,5,3,2,0) |
| $\ell$ = 15 | (6,4,3,2,0) | (2,1,0)(4,3,2,1,0) | (6,4,3,2,0) |
| $\ell$ = 9 | (6,5,3,1,0) | $(2,1,0)^3$ | (6,5,3,1,0) |
| $\ell$ = 7 | (6,5,4,3,2,1,0) | (3,1,0)(3,2,0) | (6,5,4,3,2,1,0) |
| L = 127 | (7,1,0) | | (7,6,0) |
| $\ell$ = 93 | (7,2,0) | (2,1,0)(5,4,2,1,0) | (7,5,0) |
| L = 127 | (7,3,0) | | (7,4,0) |
| L = 127 | (7,3,2,1,0) | | (7,6,5,4,0) |
| $\ell$ = 42 | (7,4,2,1,0) | $(2,1,0)^2(3,1,0)$ | (7,6,5,3,0) |
| L = 127 | (7,5,2,1,0) | | (7,6,5,2,0) |
| $\ell$ = 105 | (7,6,2,1,0) | (3,2,0)(4,1,0) | (7,6,5,1,0) |
| L = 127 | (7,4,3,2,0) | | (7,5,4,3,0) |
| $\ell$ = 105 | (7,5,3,2,0) | (3,1,0)(4,1,0) | (7,5,4,2,0) |
| $\ell$ = 93 | (7,6,3,2,0) | (2,1,0)(5,3,2,1,0) | (7,5,4,1,0) |
| $\ell$ = 35 | (7,6,4,3,0) | (3,1,0)(4,3,2,1,0) | (7,4,3,1,0) |
| L = 127 | (7,5,3,1,0) | | (7,6,4,2,0) |
| L = 127 | (7,6,3,1,0) | | (7,6,4,1,0) |
| L = 127 | (7,6,5,4,3,2,0) | | (7,5,4,3,2,1,0) |
| $\ell$ = 93 | (7,6,5,4,3,1,0) | (2,1,0)(5,2,0) | (7,6,4,3,2,1,0) |
| L = 127 | (7,6,5,4,2,1,0) | | (7,6,5,3,2,1,0) |
| $\ell$ = 63 | (8,7,0) | (2,1,0)(6,4,3,1,0) | (8,1,0) |
| $\ell$ = 30 | (8,2,0) | $(4,1,0)^2$ | (8,6,0) |
| $\ell$ = 217 | (8,3,0) | (3,1,0)(5,3,2,1,0) | (8,5,0) |
| $\ell$ = 12 | (8,4,0) | $(2,1,0)^4$ | (8,4,0) |
| $\ell$ = 217 | (8,7,6,5,0) | (3,1,0)(5,4,2,1,0) | (8,3,2,1,0) |
| $\ell$ = 15 | (8,7,6,4,0) | (4,1,0)(4,3,2,1,0) | (8,4,2,1,0) |
| $\ell$ = 63 | (8,7,6,3,0) | (2,1,0)(6,1,0) | (8,5,2,1,0) |
| $\ell$ = 217 | (8,6,2,1,0) | (3,1,0)(5,2,0) | (8,7,6,2,0) |
| L = 255 | (8,7,2,1,0) | | (8,7,6,1,0) |
| $\ell$ = 51 | (8,4,3,1,0) | | (8,7,5,4,0) |

Table II (Con't)

| Length, $\ell$ | Polynomial | Factors of Polynomial | Reverse of Polynomial |
|---|---|---|---|
| L = 255 | (8,5,3,1,0) | | (8,7,5,3,0) |
| $\ell$ = 21 | (8,7,5,2,0) | (2,1,0)(6,4,2,1,0) | (8,6,3,1,0) |
| $\ell$ = 85 | (8,7,3,1,0) | | (8,7,5,1,0) |
| L = 255 | (8,4,3,2,0) | | (8,6,5,4,0) |
| L = 255 | (8,5,3,2,0) | | (8,6,5,3,0) |
| L = 255 | (8,6,3,2,0) | | (8,6,5,2,0) |
| L = 255 | (8,7,3,2,0) | | (8,6,5,1,0) |
| $\ell$ = 217 | (8,5,4,1,0) | (3,1,0)(5,3,0) | (8,7,4,3,0) |
| $\ell$ = 217 | (8,6,4,1,0) | (3,2,0)(5,4,2,1,0) | (8,7,4,2,0) |
| $\ell$ = 30 | (8,7,4,1,0) | (2,1,0)$^2$(4,3,2,1,0) | (8,7,4,1,0) |
| $\ell$ = 63 | (8,5,4,2,0) | (2,1,0)(6,5,2,1,0) | (8,6,4,3,0) |
| $\ell$ = 10 | (8,6,4,2,0) | (4,3,2,1,0)$^2$ | (8,6,4,2,0) |
| $\ell$ = 17 | (8,5,4,3,0) | | (8,5,4,3,0) |
| $\ell$ = 85 | (8,5,4,3,2,1,0) | | (8,7,6,5,4,3,0) |
| L = 255 | (8,6,4,3,2,1,0) | | (8,7,6,5,4,2,0) |
| $\ell$ = 30 | (8,6,5,3,2,1,0) | (2,1,0)$^2$(4,1,0) | (8,7,6,5,3,2,0) |
| $\ell$ = 85 | (8,6,5,4,2,1,0) | | (8,7,6,4,3,2,0) |
| $\ell$ = 85 | (8,6,5,4,3,1,0) | | (8,7,5,4,3,2,0) |
| $\ell$ = 21 | (8,6,5,4,3,2,0) | (2,1,0)(3,1,0)(3,2,0) | (8,6,5,4,3,2,0) |
| $\ell$ = 51 | (8,7,4,3,2,1,0) | | (8,7,6,5,4,1,0) |
| $\ell$ = 217 | (8,7,6,5,3,1,0) | (3,1,0)(5,3,2,1,0) | (8,7,5,3,2,1,0) |
| $\ell$ = 42 | (8,7,6,4,3,1,0) | (2,1,0)(3,1,0)$^2$ | (8,7,5,4,2,1,0) |
| $\ell$ = 15 | (8,7,5,4,3,1,0) | (4,1,0)(4,3,0) | (8,7,5,4,3,1,0) |
| L = 255 | (8,7,6,3,2,1,0) | | (8,7,6,5,2,1,0) |
| $\ell$ = 17 | (8,7,6,4,2,1,0) | | (8,7,6,4,2,1,0) |
| $\ell$ = 9 | (8,7,6,5,4,3,2,1,0) | (2,1,0)(6,3,0) | (8,7,6,5,4,3,2,1,0) |

Using some orderly process for doing this, all n$^{th}$ degree polynomials that are factorable will appear. A useful theorem in doing this operation is the following:

Theorem 6: If any factor of a polynomial contains an even number of terms, the polynomial contains an even number of terms.

This theorem is proved in the Appendix. Using this theorem it is necessary to consider only polynomials with odd number of terms as factors when constructing, in an orderly manner, all the factorable n$^{th}$ degree polynomial with an odd number of non-zero coefficients.

Referring now to Table II and Theorem 5 above, all the polynomials in the table which do not show factors may represent generators of maximal sequences. In each case, however, there may be some irreducible polynomials which do not represent maximal sequence generators. Our remaining problem is to find some method for eliminating those irreducible polynomials which do not represent maximal sequence generators. For example, consider a generator of 6 stages. From $\frac{\phi(63)}{6}$ we know that there are 6 maximal sequences, but from Table II we see that there are 9 polynomials of the 6th degree that are irreducible. Hence three of these polynomials must be eliminated.

The procedure used for this elimination is based on the fact that, if the polynomial is irreducible then the period of the corresponding generator is equal to $2^n - 1 = L$, or it divides $2^n - 1$. Our purpose here is to separate or eliminate those whose period non-trivially divides L. The previous statement is equivalent to saying that the A matrix from a generator represented by an irreducible polynomial satisfies the equation:

$$A^L = A^{2^n - 1} = I \qquad (32)$$

A = matrix representing the generator corresponding to an irreducible polynomial.

But the statement also says that the A may satisfy an equation of the type:

$$A^{\frac{L}{k}} = I \qquad (33)$$

where: k is any number that divides L.

Since k must be a number that divides L, we may consider k to be one of the factors of L.

To determine whether a given irreducible polynomial represents a maximal generator, we have to check to see whether equation (33) is satisfied for some k. Although this procedure becomes lengthy for large n, it is not completely unwieldy. The procedure to be described for performing this check is a reasonably quick method.

First set the characteristic equation to zero, and then solve for $A^n$. Raise $A^n$ to $A^{L/k}$ (it is advisable to start with the smallest k's and proceed through the larger ones and the products), carrying out the same operation on the other side of the equation. The object then is to reduce the right side of the equation, using the equations calculated in finding $A^{L/k}$, until the right side is reduced to the minimum powers (determined by the characteristic equation). If this procedure results in $A^{L/k} = I$, then the given polynomial represents a generator whose period is equal to or divides L/k. If no k works in this process, then the polynomial must represent a maximally long sequence whose period is L.

Example 9: Consider the feedback equation [8,5,4,3,0 ]. L for n = 8 is 255, and the factors of 255 are 3, 5, and 17. From Table II we see that this feedback connection results in an irreducible polynomial; we wish to check to see whether the resulting sequence is truly maximal or if its period divides L. For this, the procedure described above is utilized. The characteristic equation for this connection is:

$$A^8 + A^5 + A^4 + A^3 + I \equiv (8, 5, 4, 3, 0) \equiv 0 \pmod 2 \qquad (34)$$

For the rest of the calculations we will use the short notation form. Dividing 255 by the smallest factor, 3, we will first check for $A^{85} = I$. We first find the equation for $A^{85}$ by repeatedly squaring the original equation[1] and then multiplying by the necessary power of A in the last step:

$$\begin{aligned} &1.\ (8, 5, 4, 3, 0)\\ &2.\ (16, 10, 8, 6, 0)\\ &3.\ (32, 20, 16, 12, 0)\\ &4.\ (64, 40, 32, 24, 0)\\ &5.\ (85, 61, 53, 45, 21)\\ &\quad A^{85} + A^{61} + A^{53} + A^{45} + A^{21} \equiv 0 \pmod 2\\ &\quad A^{85} \equiv A^{61} + A^{53} + A^{45} + A^{21} \pmod 2 \end{aligned} \qquad (35)$$

[1] Squaring a polynomial, mod 2, results in doubling the powers, since all cross product terms have a coefficient of $2 \equiv 0 \pmod 2$

We now wish to reduce the right side of the last equation; it is desired to determine whether $A^{85} = I$. To do this, we use the lower order equations of (35), multiplied by the appropriate power of A in each case:

$$\begin{array}{llr}
 & (61, 53, 45, 21) & \\
(\#3)A^{29} & + \ \underline{61, \quad 49, 45, 41, 29} & \\
 & 53, 49, 41, 29, \quad 21 & \\
(\#3)A^{21} & + \ \underline{53, \quad 41, 37, 33, 21} & (36) \\
 & 49, \quad 37, 33, \quad 29 & \\
(\#3)A^{17} & + \ \underline{49, \quad 37, 33, \quad 29, 17} & \\
 & 17 & \\
(\#2)A & + \ \underline{17, 11, 9, 7, 1} & \\
 & 11, 9, 7, 1 & \\
(\#1)A^{3} & + \ \underline{11, 8, 7, 6, 3} & \\
 & 9, 8, 6, 3, 1 & \\
(\#1)A & + \ \underline{9, 6, 5, 4, 1} & \\
 & 8, 5, 4, 3 & \\
(\#1) & + \ \underline{8, 5, 4, 3, 0} & \\
 & 0 &
\end{array}$$

$$A^{85} \equiv A^{o} \equiv I$$

From this we see that $A^{85}$ does indeed equal I; hence we know that the sequence from [8, 5, 4, 3, 0] is not 255 long, but its length divides 255 and is periodic every 85 digits. Further checking with this example will show that the period is $A^{17} = I$.

This is the method first used by the authors to eliminate those irreducible polynomials whose periods divide the maximal length L. When the proper number of such polynomials have been eliminated, all the remaining irreducible ones must represent maximal sequences. It has also been our practice, in this work, to check the mathematical results with an experimental shift register generator.

We can now summarize the steps of this method for finding the connections for an n stage generator which provide maximal sequences. 1) Consider only polynomials with an odd number of terms. 2) Take all factors of degree less than n and multiply together all combinations which produce $n^{th}$ degree polynomials. (All these will also contain only an odd number of terms). 3) Construct all the remaining $n^{th}$ polynomials with an odd number of terms. These constructed ones will all be irreducible. The number to be eliminated is equal to the difference between the value of $\frac{\phi(2^n - 1)}{n}$ and the number of irreducible equations. 4) Eliminate those irreducible polynomials which do not provide maximal sequences by the procedure described in equations (35) and (36).

### 4.2.2 Second Method

The second method for determining the maximal length connections of a given n-stage generator differs from the first in two respects: (1) one need not check a large number of possibilities in order to eliminate most polynomials (the reducible ones) to obtain the relatively few desired ones; instead one solves explicitly for the proper connections one at a time, (2) the characteristic polynomial for one maximal length generator must be known---the others will be obtained from it.

This second method makes use of the sampling idea discussed under Section 4, Theorem 4; namely, if k is relatively prime to L one maximal sequence can be derived from another by sampling every $k^{th}$ digit. If we let the matrix for the given maximal generator be A, then sampling its output sequence every k digits is equivalent to operating with the multiple-return generator $A^k$, or its simple equivalent. Thus, given one maximal generator with matrix A, one can find another maximal by finding the characteristic polynomial for $A^k$ where k is an integer relatively prime to L.

The direct way to find the characteristic polynomial for $A^k$ is to expand the determinant $|A^k + \xi I|$. Direct expansion of this determinant to find the coefficients of $\xi$ becomes difficult for large n; the method detailed below circumvents direct expansion by using the $B_A$ matrix introduced in Section 3.[1] In order to find the characteristic polynomial of the $k^{th}$ power of a maximal matrix one need only find a $nk^{th}$ degree equation that contains only those powers which are multiples of k. In this method this is accomplished by relating higher powers of A to sums of the first n powers (which is the function of the $B_A$ matrix) and obtaining the answer by inspection.

The first step in this method is to group together those powers of the given matrix which are both relatively prime to L and have the same characteristic equation. Each grouping is called a "similarity class" and is formed by repeatedly squaring (doubling the powers) of an initial entry. This process is completely formal, dealing only with powers and not with any specific matrices. (See Section 4, equation 27)

The second step is to form the $B_A$ matrix for the A matrix of the given maximal SSRG. The $B_A$ matrix was discussed in Section 3.4, page 30, together with its fairly simple construction. The power and usefulness of the $B_A$ matrix is that it relates powers of the matrix to the first few, as given by equation (21), repeated here

$$A^k = \sum_{i=1}^{n} b_{k,i} A^{n-i} \qquad (21)$$

If r is the lowest power of the similarity class for which we desire the characteristic polynomial, the $(r)^{th}$, $(2r)^{th}$, $(3r)^{th}$....$(nr)^{th}$ rows of the $B_A$ matrix are extracted. From this set of equations the $nr^{th}$ and a subset of the other rows is chosen such that the mod-2 sum of the last column is one, and the

[1] The $B_A$ matrix might also be helpful in direct expansion since the powers of SSRG matrices can be "spotted" in the $B_A$ matrix. $A^p = (b_{p+n-i,j})$

mod-2 sum of the other columns is zero. Then it is obvious that the matrices corresponding to these chosen rows add to the identity matrix:

$$A^{r.n} + A^{r.k} + - - - - A^{r.s} \equiv I \pmod{2} \tag{37}$$

The result is that the $r^{th}$ similarity class corresponds to the characteristic polynomial (n,k,----s,0) because, by equation (37), $A^r$ is a root of this polynomial. This was the desired objective: to find the characteristic polynomial of the chosen power of the original (maximal) matrix. If this technique is repeated for all similarity classes, all of the characteristic polynomials that correspond to maximal generators will be obtained.

Example 10: Consider that one wishes to find all the maximal connections for an 8 stage generator, and that we know that the generator with characteristic polynomial (8, 7, 2, 1, 0) is one of the maximal generators. The first step is to form the similarity classes for the 8 stage situation; $2^8 - 1 = 255$, and therefore the following classes appear (these are constructed exactly as previously in equation (27)). The numbers in these classes all refer to powers of A; only the powers themselves are shown in equation (38).

$$\begin{array}{ll}
\{1, 2, 4, 8, 16, 32, 64, 128\} & \{127 \ldots\ldots\ldots\} \\
\{7, 14, 28, 56, 112, 224, 193, 131\} & \{31 \ldots\ldots\ldots\} \\
\{11, 22, 44, 88, 176, 97, 194, 133\} & \{61 \ldots\ldots\ldots\} \\
\{13, 26, 52, 104, 208, 161, 67, 134\} & \{47 \ldots\ldots\ldots\} \\
\{19, 38, 76, 152, 49, 98, 196, 137\} & \{59 \ldots\ldots\ldots\} \\
\{23, 46, 92, 184, 113, 226, 197, 139\} & \{29 \ldots\ldots\ldots\} \\
\{37, 74, 148, 41, 82, 164, 73, 146\} & \{91 \ldots\ldots\ldots\} \\
\{43, 86, 172, 89, 178, 101, 202, 149\} & \{53 \ldots\ldots\ldots\}
\end{array} \tag{38}$$

It will be recalled that this table is constructed by doubling the odd numbers that are coprime to 255; when $2^8 - 1$ is reached one must begin subtracting $2^8 - 1$ from the number to complete the similarity class. For example, in the second class of 38, $(2)(193) \equiv 131 \pmod{255}$. Note that, for the 8 stage situation there should be a total of 16 similarity classes, but equation (38) shows only 8 of them; the reason for this is that the remaining 8 are related to those shown by simple reverses. Since, if we are given a maximal connection, we can quickly write the reverse, we need only consider half of the total similarity classes. In equation (38) the basic number of the similarity class which forms the reverse is shown to the right of each class. In each case this number is achieved by taking the highest number in the similarity class and subtracting it from the maximal length (255). It should be emphasized that there is a similarity class associated with each number on the right, but only the one number is written since we need consider only half the classes.

The next step is to construct the $B_A$ matrix, using the known generator condition: $A^8 = A^7 + A^2 + A + I$. The object, when constructing the $B_A$ matrix, is to express each power of A, up to the 255th power in terms of the sum of powers which are n - 1 or less. The first part of the $B_A$ matrix for the 8 stages with the given equation is shown in Figure 17. From this $B_A$ matrix we now wish to identify a polynomial with each of the classes of equation (38). The first class, of course, is associated with the given generator and the polynomial (8, 7, 2, 1, 0). For the second class we wish to find the powers in equation (37) where the r is equal to 7. We take all the multiples of 7 up through the 8th multiple and pick out the corresponding expressions from the $B_A$ matrix. This results in the group of expressions shown in Figure 17(b). As previously, each of these numbers represents a power of A: the second expression, for example, is $A^{14} = A^6 + A^5 + A^4 + A^3 + A + I$.

It is now necessary to find the unique combination of expressions which will cause all powers less than 8 to add to zero (mod. 2) except the zero power. In this step it is always necessary to use the expression for the nth multiple because we want a final equation of the nth degree. Using the last expression, then, and remembering that only the zero term must not add to zero, it is found that the unique combination of expressions is that shown in Figure (17b). Hence $A^7$ satisfies the following equation:

$$(A^7)^8 + (A^7)^7 + (A^7)^3 + (A^7)^2 + I = 0 \qquad (39)$$

$$\Rightarrow A^7 \text{ is a root of } (8,\ 7,\ 3,\ 2,\ 0) = 0$$

This means, then, that the second similarity class of equation (38) is associated with the polynomial (8,7,3,2,0) and hence with the generator [8,6, 5, 1, 0]. In this way all the maximal generators of 8 stages can be determined provided that one maximal generator is known.

It should be remarked that this last step---finding the unique combinations of expressions---is somewhat a matter of "art." Pure trial and error is of course a possibility; however, it seems plausible that a method could be devised to structure this step so that one proceeds monotonically towards the solution.

For additional clarity the expressions and final combination for the third similarity class ($A^{11}$) is given in Figure 17c while the work for

|  | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| 1 | . | . | . | . | . | . | 1 | . |
| 2 | . | . | . | . | . | 1 | . | . |
| 3 | . | . | . | . | 1 | . | . | . |
| 4 | . | . | . | 1 | . | . | . | . |
| 5 | . | . | 1 | . | . | . | . | . |
| 6 | . | 1 | . | . | . | . | . | . |
| 7 | 1 | . | . | . | . | . | . | . |
| 8 | 1 | . | . | . | . | 1 | 1 | 1 |
| 9 | 1 | . | . | . | 1 | . | . | 1 |
| 10 | 1 | . | . | 1 | . | 1 | . | 1 |
| 11 | 1 | . | 1 | . | 1 | 1 | . | 1 |
| 12 | 1 | 1 | . | 1 | 1 | 1 | . | 1 |
| 13 | . | . | 1 | 1 | 1 | 1 | . | 1 |
| 14 | . | 1 | 1 | 1 | 1 | . | 1 | . |
| 15 | 1 | 1 | 1 | 1 | . | 1 | . | . |
| 16 | . | 1 | 1 | . | 1 | 1 | 1 | 1 |
| 17 | 1 | 1 | . | 1 | 1 | 1 | 1 | . |
| 18 | . | . | 1 | 1 | 1 | . | 1 | 1 |
| 19 | . | 1 | 1 | 1 | . | 1 | 1 | . |
| 20 | 1 | 1 | 1 | . | 1 | 1 | . | . |
| 21 | . | 1 | . | 1 | 1 | 1 | 1 | 1 |
| 22 | 1 | . | 1 | 1 | 1 | 1 | 1 | . |
| 23 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 |
| 24 | . | 1 | 1 | 1 | . | . | . | 1 |
| 25 | 1 | 1 | 1 | . | . | . | 1 | . |
| 26 | . | 1 | . | . | . | . | 1 | 1 |
| 27 | 1 | . | . | . | . | 1 | 1 | . |
| 28 | 1 | . | . | . | 1 | . | 1 | 1 |
| 29 | 1 | . | . | 1 | . | . | . | 1 |
| 30 | 1 | . | 1 | . | . | 1 | . | 1 |
| 31 | 1 | 1 | . | . | 1 | 1 | . | 1 |
| 32 | . | . | . | 1 | 1 | 1 | . | 1 |
| 33 | . | . | 1 | 1 | 1 | . | 1 | . |
| 34 | . | 1 | 1 | 1 | . | 1 | . | . |
| 35 | 1 | 1 | 1 | . | 1 | . | . | . |
| 36 | . | 1 | . | 1 | . | 1 | 1 | 1 |
| 37 | 1 | . | 1 | . | 1 | 1 | 1 | . |
| 38 | 1 | 1 | . | 1 | 1 | . | 1 | 1 |
| 39 | . | . | 1 | 1 | . | . | . | 1 |
| 40 | . | 1 | 1 | . | . | . | 1 | . |
| 41 | 1 | 1 | . | . | . | 1 | . | . |
| 42 | . | . | . | . | 1 | 1 | 1 | 1 |
| 43 | . | . | . | 1 | 1 | 1 | 1 | . |
| 44 | . | . | 1 | 1 | 1 | 1 | . | . |
| 45 | . | 1 | 1 | 1 | 1 | . | . | . |
| 46 | 1 | 1 | 1 | 1 | . | . | . | . |
| 47 | . | 1 | 1 | . | . | 1 | 1 | 1 |
| 48 | 1 | 1 | . | . | 1 | 1 | 1 | . |
| 49 | . | . | . | 1 | 1 | . | 1 | 1 |
| 50 | . | . | 1 | 1 | . | 1 | 1 | . |
| 51 | . | 1 | 1 | . | 1 | 1 | . | . |
| 52 | 1 | 1 | . | 1 | 1 | . | . | . |

(a) $B_A$ matrix (up to $A^{52}$) for (8,7,2,1,0)

| n | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | n | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 1 | . | . | . | . | . | . | . |  |  |  |  |  |  |  |  |  |  |
| 14 | . | 1 | 1 | 1 | 1 | . | 1 | . | 2·7 | . | . | 1 | 1 | 1 | 1 | . | 1 | . |
| 21 | . | 1 | . | 1 | 1 | 1 | 1 | 1 | 3·7 | . | . | 1 | . | 1 | 1 | 1 | 1 | 1 |
| 28 | 1 | . | . | . | . | 1 | 1 | . |  |  |  |  |  |  |  |  |  |  |
| 35 | 1 | 1 | 1 | . | 1 | . | . | . |  |  |  |  |  |  |  |  |  |  |
| 42 | . | . | . | . | 1 | 1 | 1 | 1 |  |  |  |  |  |  |  |  |  |  |
| 49 | . | . | . | 1 | 1 | . | 1 | 1 | 7·7 | . | . | . | . | 1 | 1 | . | 1 | 1 |
| 56 | . | . | 1 | 1 | 1 | 1 | 1 | 1 | 8·7 | . | . | . | 1 | 1 | 1 | 1 | 1 | 1 |

(b)

Those expressions from the $B_A$ matrix, which specify the polynomial corresponding to the 2nd similarity class of equation (38)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11 | 1 | . | 1 | . | 1 | 1 | . | 1 | 1·11 | . | 1 | . | 1 | . | 1 | 1 | . | 1 |
| 22 | 1 | . | 1 | 1 | 1 | 1 | 1 | . | 2·11 | . | 1 | . | 1 | 1 | 1 | 1 | 1 | . |
| 33 | . | . | 1 | 1 | 1 | . | 1 | . | 3·11 | . | . | . | 1 | 1 | 1 | . | 1 | . |
| 44 | . | . | 1 | 1 | 1 | 1 | . | . | 4·11 | . | . | . | 1 | 1 | 1 | 1 | . | . |
| 55 | 1 | 1 | . | 1 | 1 | 1 | . | . |  |  |  |  |  |  |  |  |  |  |
| 66 | . | 1 | . | 1 | . | 1 | 1 | . | 6·11 | . | . | 1 | . | 1 | . | 1 | 1 | . |
| 77 | 1 | 1 | . | . | 1 | . | 1 | . |  |  |  |  |  |  |  |  |  |  |
| 88 | . | 1 | . | . | . | . | 1 | . | 8·11 | . | . | 1 | . | . | . | . | 1 | . |

(c)

Those expressions which specify the polynomials for the 3rd similarity class of equation (38)

Figure 17: Illustrating the method for identifying the polynomial corresponding to the similarity classes of equation (38).

the remaining similarity classes is in Appendix B.

Finally, Figure 18 shows the similarity classes with all the associated polynomials which specify the maximal generators. Each of these generators has a reverse (it can be shown that for n > 2, no maximal is self-reverse) and this total number of generators represent all the simple generators of 8 stages that can produce maximal sequences.

| Similarity Powers | Char. Eqn. | Lowest Power of Reverse |
|---|---|---|
| {1,2,4,8,16,32,64,128} | (8,7,2,1,0) | 127 |
| {7,14,28,56,112,224,193,131} | (8,7,3,2,0) | 31 |
| {11,22,44,88,176,97,194,133} | (8,6,4,3,2,1,0) | 61 |
| {13,26,52,104,208,161,67,134} | (8,6,3,2,0) | 47 |
| {19,38,76,152,49,98,196,137} | (8,7,5,3,0) | 59 |
| {23,46,92,184,113,226,197,139} | (8,5,3,2,0) | 29 |
| {37,74,148,41,82,164,73,146} | (8,7,6,5,2,1,0) | 91 |
| {43,86,172,89,178,101,202,149} | (8,6,5,4,0) | 53 |

Figure 18: The similarity classes and their associated polynomials for 8-stage maximal generators

This then completes the consideration of the second method for finding those connections of an n-stage generator which provide maximal length sequences. Both of the methods described become quite lengthy and laborious when the number n becomes large. However, for any extended work of this type a digital computer program could be written to find the solutions. Also, it is felt that the second method offers a unique advantage over the first: if only a certain number and not all of the proper connections are desired, the work for the second method is reduced (the $B_A$ matrix has only to be completed to corresponding order). In the first method one must eliminate all the undesired irreducible polynomials before one is sure of obtaining any sizable number of proper generators. This makes the second of the two methods described somewhat more attractive.

### 4.3 Sequences from Multiple-Return Generators

We have now dealt with the two questions of how many maximal sequences exist for an n stage generator, and how are the proper connections which provide the maximal sequences determined. In the previous sections we have implicitly been considering only simple generators. It appears pertinent to ask whether multiple-return generators provide any additional maximal sequences, or whether their maximal sequences are different than those from the simple generators.

The answer is negative to both of these questions. It was stated in Section 1 that every multiple-return generator (that has no transients) has an equivalent simple generator. We shall consider now the reason for this. Consider a multiple-return generator and its A matrix. One can now find the companion matrix associated with the characteristic equation of the A matrix. Having found this companion matrix one has specified in effect the equivalent simple generator. If one wires a generator according to this companion matrix, the generator will provide the sequences of the original one, and it is a simple one.

For these reasons we will not achieve new sequences from multiple-return generators. This is not to say that multiple-return generators are of no importance. They may well have useful applications, such as obtaining a number of sequences from the same generator without reloading, for example.

### 4.4 Shift and Add Property

An important property of maximal sequences is the shift and add property. In Section 2 it was stated that the shift and add property implies that, when a sequence is added to a shifted version of itself in a modulo-two fashion, the resulting sequence is in turn a shifted version of the original sequence. We can now state this in a more precise fashion:

Definition: A sequence is said to have the shift and add property if, for every integer m there exists an integer f(m) such that:

$$A^m + A^{f(m)} \equiv I \qquad \text{(mod 2)} \qquad (40)$$

where A = matrix for the simple generator of the sequence.

We now wish to show that every maximal sequence has the shift and add property.

In the Appendix, Lemma 6 states: "Any shift and add sum of digits of a sequence obeys that sequence's laws." That is to say, if a sequence is shifted and added to itself, the resulting sequence will obey the same sequence laws as the original one. The proof is also given in the Appendix. Now if the original sequence was a maximal sequence, then one and only one sequence can be generated using its characteristic sequence law. Hence if the shift and add sequence obeys the same characteristic sequence law, it itself must be the same maximal sequence.

This is the proof, then, that every maximal sequence has the shift and add property.

### 4.5 Auto-correlation

Another important property of digital sequences is their auto-correlation and this property, because of the definition of auto-correlation is related very closely to the shift and add property described above. In many applications of digital sequences the auto-correlation function should be of a particular type; we shall show here that all maximally long sequences have a distinctive auto-correlation function.

The auto-correlation for a general given waveform x(t) with no d-c component is defined as:

$$\rho(k) = \lim_{T \to oo} \frac{\int_{-T}^{T} x(t)\, x(t+k)\, dt}{\int_{-T}^{T} x^2(t)\, dt} \qquad (41)$$

where p(k) = auto-correlation function for the waveform x(t). If the waveform has a period T we need not consider this limiting process, and the definition becomes

$$\rho(k) = \frac{\int_{o}^{T} x(t)\, x(t+k)\, dt}{\int_{o}^{T} x^2\, (t)\, dt} \qquad (42)$$

Since digital sequences are periodic, this is the appropriate definition.

In the past we have considered the digital sequence as consisting of a series of 0's or 1's. Hence the associated waveform that we think of consists of a square wave that alternates between a 0 value and a 1 value. We have to alter this conception a bit now, since for purposes of considering auto-correlation we do not want a d-c component in the wave. For this reason, we shall think of the sequence as consisting of either +1's or -1's; such a wave will not have an appreciable d-c component (at least in the maximally long case). We will neglect this slight d-c component and use the +1 and -1 representation to find the auto-correlation.

Since we have a square wave, we can write the integral of equation (42) as a summation:

$$\rho(k) = \frac{\sum_{j=1}^{L} x(j)\, x(j+k)}{\sum_{j=1}^{L} x^2(j)} = \frac{1}{L} \sum_{j=1}^{L} x(j)\, x(j+k) \qquad (43)$$

ρ(k) = digitized auto-correlation of digital sequence

k = integer, corresponding to shifts of a sequence generator.

To evaluate this equation we can think of the positive and the negative areas that result when two shifted sequences are multiplied together. This is most easily done by comparing the multiplication table for +1 and -1 with the modulo-two addition table for a 1 and a 0. Figure 19 shows these two tables side by side for comparison:

Modulo-Two Addition

|   | 1 | 0 |
|---|---|---|
| 1 | 0 | 1 |
| 0 | 1 | 0 |

Arithmetic Multiplication

|    | +1 | -1 |
|----|----|----|
| +1 | +1 | -1 |
| -1 | -1 | +1 |

Figure 19. Comparing Modulo-Two Addition for a 1 and 0 With Multiplication for +1 and -1

Choose for a moment a given value of k in equation (43); we then wish to evaluate the summation in this equation. From Figure 19 we see that the summation consists of a series of +1's and -1's, and that we can consider this in turn to be a digital sequence. Using equation (43), it is seen that $\rho(k)$ can be written:

$$\begin{aligned}\rho(k) &= \frac{1}{L}\,(\text{number of matching digits} - \text{number of differing digits}) \\ &= \frac{1}{L}\,(L - 2 \times \text{numbers of differing digits}) = \frac{L - 2d}{L} \qquad (44)\end{aligned}$$

Further, the summation of equation (43) can be regarded as the result of modulo-two adding the two shifted sequences with the proviso that a +1 corresponds to a 0, and a -1 corresponds to a 1. Then using our prior knowledge about the shift and add properties of maximal sequences, we know how many +1 areas exist in the summation. The shift and add property states that the same sequence is returned if maximally long sequences are involved. Based on this, then, there are $\frac{L+1}{2}$ ones and $\frac{L-1}{2}$ "minus ones" in the product sequence of equation (43).

The auto-correlation then, for any value of k not equal to 0, is:

$$\rho(k \neq 0) = \frac{L - (L + 1)}{L} = \frac{-1}{L} \qquad (45)$$

$$\rho(o) = \frac{L}{L} = 1 \qquad (46)$$

Equation (45) and (46) then give the value for the auto-correlation for any maximally long digital sequence. The correlation is always 1 for zero shift, and drops to -1/L for any other shift. As L increases (with large n), the correlation function becomes closer and closer to an ideal; it would be ideal if the value were 1 for zero shift and zero for all other shifts.

If one rigorously accounts for the remaining slight d-c component of the $\pm 1$ waveform, one should replace L by $(L - \frac{1}{L})$ in the final expression of (44), and L by (L - 1) in equation 45.

Sequences with a general period P have been called "perfect sequences" if the auto-correlation for non-zero shift is no more than $\pm$ 1/P-1. It has been shown here that all of the maximal length sequences from linear SRG's are perfect sequences. This concludes our consideration of maximally long sequences.

## SECTION 5: NON-MAXIMAL SEQUENCES

In this section non-maximal sequences are treated in the same manner as maximal sequences were treated in the previous section. The purpose here is to consider any structure that we have found in non-maximal sequences, and to use the mathematical tools developed in Section 3 to deal with this structure. The two major topics for discussion will be consideration of how many sequences will occur for a given non-maximal connection, and what shift and add properties are exhibited by non-maximal sequences.

## 5.1 Number and Lengths of Non-Maximal Sequences

It will be recalled that a non-maximal feedback connection generates a set of sequences (Section 2 page 10). Consider the question of the number of sequences and their lengths for a given non-maximal connection. The characteristic polynomials for each connection can be used for this purpose. These polynomials fall into one of three categories: (1) the polynomial is irreducible, (2) the polynomial is reducible, but there are no repeating factors, and (3) the polynomial is reducible and there are repeating factors. The three cases will be treated in order.

If the polynomial is irreducible, all the sequences will be of the same length, and hence the number of sequences must be a factor of $L = 2^n - 1$. At present we know of no way to predict which of the possible numbers is the correct one from the connections alone. Our practice has been to determine the order of the A matrix using the procedure described in equations (35) and (36). When the lowest order of the A matrix has been found, this order divided into the value of L gives the number of sequences. For an illustration, consider the example treated previously where the feedback equation is [8, 5, 4, 3, 0].(Section 2, page44). After using the procedure to find the order of the matrix, it was found that the lowest order was 17. Hence, for this SRG there are 15 sequences all of length 17. Of course the IR response sequence is one of these 15.

### 5.1.1 Factorable Characteristic Polynomials

When the polynomials that represent a non-maximal SRG are factorable, the number of sequences (and their lengths) can be determined by considering the factors themselves. There are three principles which are useful in this respect and these apply to the cases of both repeated and non-repeated factors.

Principle No. 1. Theorem 2 of Section 2 states that the length of any sequence (from a given generator) divides the length of the IR sequence. Hence the length of the IR sequence for a given generator is an important piece of information.

Principle No. 2 will be stated as a theorem:

Theorem 7: Given an SSRG with a factorable characteristic polynomial, the sequences corresponding to each factor will be among the sequences of that SSRG.

By "sequences corresponding to each factor" we mean the sequence from the SSRG whose characteristic equation is that factor. Thus, given the factors of the polynomial, we can immediately identify some of these sequences---those that belong to the factors themselves. Note also that the sequence corresponding to any grouping of the factors must also appear since this too can be considered a factor.

Principle No. 3 is suggested by the above theorem. It is a physical representation of a non-maximal SRG whose characteristic polynomial is factorable. This principle consists of considering each factor as representing a separate generator, and cascading the resulting generators, as the factors themselves are cascaded in the equation. Figure 20 illustrates this representation of a generator whose polynomial is factorable. Each generator in the cascaded group has its feedback connections made according to the terms in the corresponding factor. The object of this representation is to view the generation of the entire set of sequences from the total generator as

polynomial = (n, j, ----) = (k, m, ----)(p, n, ----)(s, t, ----) ---

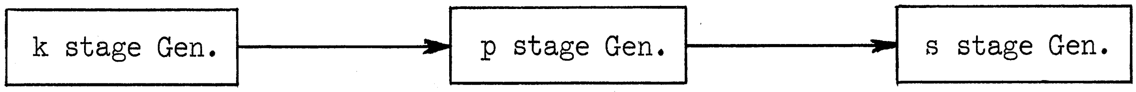


Figure 20. Physical Interpretation of a generator whose Polynomial is Factorable

stemming from different combinations of factor-generator sequences. In this process the individual generators are allowed to take on all their possible sequences including the all-zero sequence. It has been observed that this representation is valid, and it serves as a useful means for considering the set of sequences from a factorable non-maximal generator.

These principles can now be used to treat the number and the length of the set of sequences available from a factorable non-maximal generator. When the polynomial of a generator is factorable two conditions are possible: (1) the polynomial contains no repeated factors, and (2) the polynomial does contain repeated factors. The case of non-repeated factors will be considered first.

### 5.1.2 Polynomials with No Repeated Factors

Given that a polynomial has no repeated factors, the numbers and lengths of the sequences are influenced by the nature of the factors; that is, the sequences depend on whether the orders of the factors are prime to each other, and whether or not the factors themselves represent maximal generators (or non-maximal ones). We shall begin with the simplest case-----where the orders of the factors are prime to each other and the factors are maximal ones-----and then consider the alterations which are necessary when this is not the case.

Under these conditions then, we first consider how to determine the length of the impulse response sequence. It has been found that the length of the IR sequence is equal to the least common multiple of the IR lengths of the factors. It is remembered that the IR length is L for maximal factors, and $\ell$ for non-maximal ones. Hence, if a polynomial has the factors:

$$(k,m,-----)\ (p,r,-----)\ (s,t,-----) \qquad (47)$$

and if the IR response length of these factors are, respectively $\ell_1$, $\ell_2$, and

3, then the IR sequence length ($\ell$) of the product is:

$$\ell = \text{least common multiple of } (\ell_1, \ell_2, \ell_3) \tag{48}$$

Note that equation (48) is true for all polynomials that have non-repeated factors, no matter whether the $l_i$ are relatively prime or not, and whether the factors are maximal or not. Using equation (48) to find the length of the IR sequence, and using the above three principles, we can proceed to find the number of sequences and their lengths for the non-repeated factor case where the IR lengths of the factors are relatively prime and the factors are maximal.

If the IR lengths of the factors are relatively prime to each other, and the factors represent maximal SRG's, than the total number of sequences is the number of different terms that can be formed by multiplying factors together. This means that one sequence corresponds to multiplying all the factors together (this is the IR sequence), one sequence corresponds to each factor appearing alone (this comes directly from Theorem 7), and one sequence corresponds to each term that can be formed by multiplying numbers--lying between all factors and single factors----of factors together. If there are two factors in the polynomial then sequences will correspond to the following terms:

1. $(P_1)(P_2) = \ell$
2. $P_1$ (49)
3. $P_2$ where P = length of the factor sequences

The first sequence is the IR sequence and its length is the product of the individual periods. The lengths of the other two sequences are, of course, identical to the lengths of the sequences from the factors.

For the polynomial with three factors, sequences correspond to the following terms:

$$\begin{aligned}
&1.\quad P_1P_2P_3 = \ell \\
&2.\quad P_1P_2 \\
&3.\quad P_2P_3 \\
&4.\quad P_1P_3 \\
&5.\quad P_1 \\
&6.\quad P_2 \\
&7.\quad P_3
\end{aligned} \tag{50}$$

It is seen that there are seven sequences; the lengths of each of these seven is given by the products of the periods which make up the corresponding term.

Remembering that the P's are lengths of the maximal length factors, by use of Theorem 1, corollary 2 and the two preceding equations we find that

$$\begin{aligned}
L &= \ell + P_1 + P_2 && \text{(first case)} \\
L &= \ell + P_1P_2 + P_2P_3 + P_1P_3 + P_1 + P_2 + P_3 && \text{(second case)}
\end{aligned} \tag{51}$$

Example 11: Consider the generator with characteristic polynomial (8,3,0). The factors are (3,1,0) and (5,3,2,1,0). Both of these are maximal length factors and their IR lengths are relatively prime. Hence, by equation (49) there are three sequences; one is 217 long, one is 31 long, and one is 7 long.

The above example and statements are seen by considering the cascading of generators, as shown in Figure 20. From each generator, corresponding to a factor, two possible sequences can be obtained: the normal sequence and the all-zero sequence (this latter is equivalent to turning the particular generator off). Since one can arrange the factor generators in any order, one can always place a "turned-off" generator at the front. If one does this, and turns off first one generator, then two generators, etc., the above statements seem entirely plausible.

In the above way, then, the number of sequences and their lengths can be determined for the set of sequences from a non-maximal generator whose polynomial has no repeated factors, and where the IR lengths of the particular factors are relatively prime to each other and the factors themselves are maximal. We now consider what alterations are necessary when the factors themselves are non-maximal.

If some or all of the factors represent non-maximal SRG's, then subsequences will be formed within the "terms" of equations (49) and (50). It is still profitable to form the terms as in (49) and (50); now, however, each term will contribute a number of sequences instead of only one. Note that we have defined the P's to be equal to the respective L's of the factors; that is, even though a factor may be non-maximal, the P for that factor is the length of the sequence if the factor were maximal. Consider equation (49) and suppose the $P_1$ factor is non-maximal and has k non-maximal sequences. Then the following sequences and lengths will result from this two-factor generator.

| Terms | No. of Seq's | Length of Sequences | |
|---|---|---|---|
| $P_1P_2$ | k | $\frac{P_1P_2}{k}$ | |
| $P_1$ | k | $\frac{P_1}{k}$ | (52) |
| $P_2$ | 1 | $P_2$ | |

Example 12: Consider the generator (7, 4, 3, 1, 0) = (3, 2, 0) (4, 3, 2, 1, 0). The IR length of factor one is 7, and of factor two is 5; $P_1 = 7$, $P_2 = 15$. There are 3 sequences each of length 5 from the generator (4, 3, 2, 1, 0). The following sequences are obtained:

| Terms | No. of Seq's | Length of Sequences | |
|---|---|---|---|
| $P_1P_2$ | 3 | 35 | |
| $P_1$ | 1 | 7 | (53) |
| $P_2$ | 3 | 5 | |

A third situation occurs when the factors are maximal, but the IR length of these factors are not prime to each other. As in the previous case, the result is that the terms constructed in equations (49) and (50) will themselves furnish several sequences. It is still desirable to construct terms in the same fasion. Following this, the general rule to consider is that, in each case, the length of the sequences, which a particular term will provide, will be determined by the least common multiple of the IR lengths of the factors which contribute to that term. This can be illustrated by an example.

Example 13: Consider the polynomial (8,6,5,4,3,0) = (2,1,0)(3,2,0)(3,1,0). Here there are three factors, and hence the terms shown in equation (50) will appear. The IR lengths of the factors here are, respectively 3,7, and 7. Note that the last two factors are reverses; hence their sequences will be reverses. Using equation (48), the IR sequence is found to be of length 21. Therefore the length of every sequence must divide 21. We will now look successively at the terms of equation (50) and determine the sequences from each term. From term 1,($P_1P_2P_3$) we see that the product of the IR lengths is 147; but no sequence can have length greater than 21 (the IR sequence appears in the group from this term). Also the least common multiple of the IR lengths of this term is 21; therefore this term contributes 7 sequences, each of length 21. The third term contributes 7 sequences each of length 7: the l.c.m. is 7 and the product of IR lengths is 49. These terms and the number of sequences of each length are shown in equation (54).

| | Term | No. of Seq's | Length of Seq's | |
|---|---|---|---|---|
| | $P_1P_2P_3$ | 7 | 21 | |
| | $P_1P_2$ | 1 | 21 | |
| $P_1 = 3$ | $P_2P_3$ | 7 | 7 | |
| $P_2 = 7$ | $P_1P_3$ | 1 | 21 | (54) |
| $P_3 = 7$ | $P_1$ | 1 | 3 | |
| | $P_2$ | 1 | 7 | |
| | $P_3$ | 1 | 7 | |

If a combination of the two previous situations occurs----the IR lengths of the factors are not relatively prime, and the factors are not maximal length---; then a combination of the two preceding methods is employed. A good procedure is to first note the sequences which would occur if the factors were maximal (as in equations 54) and then break these terms down further as was done in equations (52) and (53).

This concludes then the determination of the number of sequences and their lengths when the polynomial is factorable but has no repeated factors. Another interesting physical interpretation can be given for this case of non-repeated roots (in addition to the interpretation of Figure 20) which is suggested by equations (49) and (50). This consists of viewing the sequences from the factors as "beating" to form the sequences of the total generator (whereas the conception of Figure 20 considers the factors as cascaded generators). By beating we mean to take all the possible sequences (including the all zero sequence) from any given factor and modulo-two add it to all the possible sequences from the other factors. For a general polynomial, this concept is depicted in Figure 21. Careful thought will show that there will be a sequence (or sequences) from this beat type

$(n,o,----) = (k,m,----)(p,r,----)(s,t,----)$

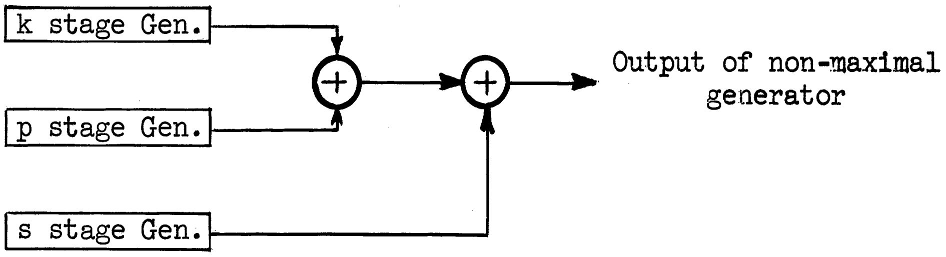


Figure 21. Concept of "Beating" the Factor Generators of a Non-Maximal Generator when the Factors are Non-Repeating

generator corresponding to every term of equations (49) and (50).

It must be noted that this beating concept applies only to the case where the factors of the polynomial are non-repeating. We shall see that the beating concept does not work when there are repeated factors.

### 5.1.3 Polynomials with Repeated Factors

We now consider the case of repeated factors. We know that the sequence corresponding to the factor itself will be included. We will in addition show that the concept of cascading, as shown in Figure 20, is still valid but the beating concept of Figure 21 is not.

As in other areas of mathematics it appears that the case of repeated factors represents a singular case. When the polynomial contains repeated factors, that generator will possess a great number of relatively short sequences. Table III of the next page shows the number and the lengths of sequences that can be obtained from a generator associated with a repeated-factor polynomial. This table includes those polynomials obtained by raising the maximal factors (2,1,0),(3,1,0), and (4,1,0) to every power up to the tenth power. It is important to note that, for a particular factor, the sequences from a given generator consist not only of the ones listed to the right of the polynomial, but also of all those which precede it (for that particular factor). The reason for this is obvious-----given a factor raised to a certain power, that factor raised to all lesser powers constitute factors of the former, and hence by Theorem 7 the sequences of this latter must appear. For this reason the third column of Table III is termed "the number of additional sequences," meaning additional to the preceding sequences. For example, the total number of sequences and their lengths available from the generator whose polynomial is $(12, 10, 6, 2, 0) = (2, 1, 0)^6$ is: 160 sequences of length 24; 20 sequences of length 12; one sequence of length 6; and one sequence of length 3.

One striking fact exhibited by Table III is that when a given factor is raised to one more power, the new sequences that are achieved (new in the respect that they did not occur in previous powers) are all of the greatest possible length. The contents of this table can be expressed by the following relation: let the repeated-factor polynomial be written: $(m,---o)^e$

Table III

No. of Sequences and their Lengths for Repeated-Factor Polynomials.

| Polynomials | Number of Additional Sequences | Length |
|---|---|---|
| $(2,1,0)$ | 1 | 3 |
| $(2,1,0)^2 = (4,2,0)$ | 2 | 6 |
| $(2,1,0)^3 = (6,5,3,1,0)$ | 4 | 12 |
| $(2,1,0)^4 = (8,4,0)$ | 16 | 12 |
| $(2,1,0)^5 = (10,9,8,6,5,4,2,1,0)$ | 32 | 24 |
| $(2,1,0)^6 = (12,10,6,2,0)$ | 128 | 24 |
| $(2,1,0)^7 = (14,13,11,10,8,7,6,4,3,1,0)$ | 512 | 24 |
| $(2,1,0)^8 = (16,8,0)$ | 2,048 | 24 |
| $(2,1,0)^9 = (18,17,16,10,9,8,2,1,0)$ | 4,096 | 48 |
| $(2,1,0)^{10} = (20,18,16,12,10,8,4,2,0)$ | 16,384 | 48 |
| | | |
| $(3,1,0)$ | 1 | 7 |
| $(3,1,0)^2 = (6,2,0)$ | 4 | 14 |
| $(3,1,0)^3 = (9,7,6,5,2,1,0)$ | 16 | 28 |
| $(3,1,0)^4 = (12,4,0)$ | 128 | 28 |
| $(3,1,0)^5 = (15,13,12,7,5,4,3,1,0)$ | 512 | 56 |
| $(3,1,0)^6 = (18,14,12,10,4,2,0)$ | 4,096 | 56 |
| $(3,1,0)^7 = (21,19,18,17,14,12,11,10,7,4,2,1,0)$ | 32,768 | 56 |
| $(3,1,0)^8 = (24,8,0)$ | 262,144 | 56 |
| $(3,1,0)^9 = (27,25,24,11,9,8,3,1,0)$ | 1,048,576 | 112 |
| $(3.1.0)^{10} = (30,26,24,14,10,8,6,2,0)$ | 8,388,608 | 112 |

Table III (Con't)

| Polynomials | Number of Additional Sequences | Length |
|---|---|---|
| $(4,1,0)$ | 1 | 15 |
| $(4,1,0)^2 = (8,2,0)$ | 8 | 30 |
| $(4,1,0)^3 = (12,9,8,6,4,3,2,1,0)$ | 64 | 60 |
| $(4,1,0)^4 = (16,4,0)$ | 1,024 | 60 |
| $(4,1,0)^5 = (20,17,16,8,5,1,0)$ | 8,192 | 120 |
| $(4,1,0)^6 = (24,18,16,12,8,6,4,2,0)$ | 131,072 | 120 |
| $(4,1,0)^7 = (28,25,24,22,20,19,18,17,13,10,9,7,5,3,2,1,0)$ | 2,097,152 | 120 |
| $(4,1,0)^8 = (32,8,0)$ | 33,554,432 | 120 |
| $(4,1,0)^9 = (36,33,32,12,9,8,4,1,0)$ | 268,435,456 | 240 |
| $(4,1,0)^{10} = (40,34,32,16,10,2,0)$ | 2,147,483,648 | 240 |

and let $k = 0,1,2,$ ......... Then the length of the <u>additional</u> sequences obtained, when the exponent is increased from $e - 1$ to $e$ is

$$\ell = (2^m-1)2^k \text{ for all } e \text{ such that } 2^{k-1} < e \leq 2^k. \qquad (55)$$

A SSRG with the polynomial $(m,\text{------}0)^e$ will generate all of the sequences of the SSRG with polynomial $(m,\text{-----})^{e-1}$ plus the set of new sequences, and these new sequences are all of length given by equation (55). There are $\frac{2^{me}\,[1-2^{-m}]}{\ell}$ of these new sequences. These relations describe the contents of Table III.

Table III exhibits the case where maximal factors are raised to some power. If the basic factor were non-maximal (they would be irreducible, or also could be factored further) then the contents of Table III would be altered in a simple way: the number of new sequences would be multiplied by the number of sequences available from the basic factor, and the length of the various new sequences would be divided by this same number.

### 5.1.4 Using the $B_A$ Matrix

Thus far we have dealt with non-maximal generators by considering the factors of their polynomials. Another means for dealing with non-maximal sequences consists of using the $B_A$ matrix, which was introduced in Section 3. The $B_A$ matrix is formed by using the characteristic equation to successively write all the powers of A in terms of the first n - 1 powers of A. This process was illustrated in Section 3. equation (23). The $B_A$ will be an $\ell$ x n matrix. If we read the $j^{th}$ column of this matrix we obtain the sequence which results from a simple generator with a single one in the $j^{th}$ position. If the generator were a maximal length one the resulting sequence would be the only possible one. For the non-maximal case considered here, however, the resulting sequences will be the elementary ones due to the single ones in the initial load: these elementary sequences will be the IR sequence if either the first or the last columns are read (corresponding to a single initial one in either the first or the last stage of a simple SRG). The important point here is that all sequences of the non-maximal SRG can be obtained by adding the various columns of the $B_A$ matrix two at a time, three at a time, etc. This process is continued until all the n-tuples have occurred in the resulting sequence. In this manner all the possible sequences from the non-maximal generator will be obtained.

Consider as an example the same generator and $B_A$ matrix that was treated earlier, in equation (23). The generator is [4,2,0] and the IR length is 6. Equation (56) repeats the $B_A$ matrix for this case.

$$B_A \quad = \quad \begin{bmatrix} 0\,0\,1\,0 \\ 0\,1\,0\,0 \\ 1\,0\,0\,0 \\ 0\,1\,0\,1 \\ 1\,0\,1\,0 \\ 0\,0\,0\,1 \end{bmatrix} \qquad (56)$$

Any column of this is the sequence resulting from a single one in the corresponding stage of the register.

Consider the response from an initial one in the 4th and in the 3rd place. Adding these gives the result:

$$\begin{array}{ll} 4^{th} \text{ place:} & 0\;0\;0\;1\;0\;1 \\ 3^{rd} \text{ place:} & \underline{1\;0\;0\;0\;1\;0} \\ \text{Result} & 1\;0\;0\;1\;1\;1 \end{array} \qquad (57)$$

This is another 6 long sequence that the register provides. A 1 in the 4th and in the 2nd place gives:

$$\begin{array}{ll} 4^{th} \text{ place:} & 0\;0\;0\;1\;0\;1 \\ 2^{nd} \text{ place:} & \underline{0\;1\;0\;1\;0\;0} \\ \text{Result} & \overline{0\;1\;0\;0\;0\;1} \end{array} \qquad (58)$$

This sequence is the same as the first and last column of equation (56), and hence is an IR sequence. If we try a 1 in the 3rd and 2nd position, we obtain:

$$\begin{array}{ll} 3^{rd} \text{ place:} & 1\;0\;0\;0\;1\;0 \\ 2^{nd} \text{ place:} & \underline{0\;1\;0\;1\;0\;0} \\ \text{Result} & \overline{1\;1\;0\;1\;1\;0} \end{array} \qquad (59)$$

This is a 3-long sequence. We now have obtained two 6-long and one 3-long sequence; these total to 15, and hence we know we have obtained all the sequences that are possible from this 4 stage non-maximal generator.

This illustrates how the $B_A$ matrix can be used to find the actual sequences that can be produced by a given non-maximal generator. The work required to form the $B_A$ matrix is somewhat lengthy, however; and it is felt that the polynomial's factors are more useful for this purpose.

### 5.2 Shift and Add Properties of Non-maximal Sequences

In the previous sections we have dealt with the question of the number and length of sequences from a non-maximal shift-register generator.

Parallel to the case of maximal sequences, an interesting property of non-maximal ones is the shift and add property. In general we can say that non-maximal sequences exhibit "partial" shift and add properties. By this we mean that, for certain shifts the shift and add property is exhibited. For the other shifts, however, a different sequence of the same SSRG is obtained. Further, it has been observed that, for certain sequences there exists a matrix which relates the sequences from one generator together and that, through this matrix, there exists a relation between non-maximal and maximal generators. We have chosen to call this matrix the C matrix; its construction will be illustrated in this section.

The shift and add properties of non-maximal sequences differ according to the factor properties of the polynomial. As noted before the three major categories are (1) the polynomial is irreducible, (2) the polynomial is factorable but contains no repeated factors, and (3) the polynomial does contain repeated factors. We will consider the categories in the order which they are listed.

### 5.2.1 Irreducible Polynomials

If the polynomial is irreducible all possible sequences are of the same length and equal to the length of the IR sequence. If one of these sequences is chosen, by shifting and adding this sequence to itself (as shown previously in Figure 9) all of the other sequences of the group will be obtained as all possible shifts are taken. The original sequence itself (shifted) will also appear for certain shifts. One can determine which shifts produce the original sequence by finding certain "basic" shifts and then successively doubling these until the resulting shifts begin to repeat mod. $\ell$. This doubling is equivalent to squaring the powers of A, and hence determining the set of permissible shifts from the basic shifts is identical to the grouping process treated earlier in equation (27). The determination of the basic shifts is the critical step in finding the permissible shifts. For this, it is convenient to consider two cases: (1) the generator has only two feedback taps, and (2) the generator has more than two feedback taps.

If the non-maximal generator has only two taps, its characteristic equation contains the two basic shifts. These two are obtained by taking each power of A in the characteristic equation plus the identity term; this is permissible since modulo-two addition is involved. Consider the generator [9,8,0] with its characteristic equation (9,1,0). The two equations which specify the basic shifts are:

$$(A + I)U = A^9U$$

and

$$(A^9 + I)U = AU \qquad (60)$$

Hence, the two basic shifts are 1 and 9. By doubling successively each of these numbers, it will be verified that the following shifts are all permissible: (61)

$$\text{shifts} = \left\{1,2,4,8,16,32,64,128 \equiv 55 (\text{mod } 73),\ 37;\ 9,18,36,72,71,69,65,57,41\right\}$$

That is, if a sequence from a generator whose polynomial is irreducible is chosen, it will be found that the shifting and adding of this sequence using the shifts obtained in the above manner, results in a shifted version of the same sequence. Other shifts of this same sequence will produce other sequences from the group of all possible sequences.

When the generator has more than two taps, it is necessary to use the $B_A$ matrix to find all the basic shifts. Given the $B_A$ matrix, one must look for two situations: (1) the case where a power of A is equal to the identity plus another power of A, and (2) the case where any two rows of the $B_A$ matrix differ only by the identity term. Consider the generator

[6,5,4,2,0] whose characteristic equation is (6,4,2,1,0). The $B_A$ matrix for this generator, obtained by the procedure of (Section 3.4) equation (22), is:

$B_A$ Matrix

$$\begin{array}{r cccccc}
 & 5 & 4 & 3 & 2 & 1 & 0 \\ \hline
1 & . & . & . & . & 1 & . \\
2 & . & . & . & 1 & . & . \\
3 & . & . & 1 & . & . & . \\
4 & . & 1 & . & . & . & . \\
5 & 1 & . & . & . & . & . \\
6 & . & 1 & . & 1 & 1 & 1 \\
7 & 1 & . & 1 & 1 & 1 & . \\
8 & . & . & 1 & . & 1 & 1 \\
9 & . & 1 & . & 1 & 1 & . \\
10 & 1 & . & 1 & 1 & . & . \\
11 & . & . & 1 & 1 & 1 & 1 \\
12 & . & 1 & 1 & 1 & 1 & . \\
13 & 1 & 1 & 1 & 1 & . & . \\
14 & 1 & . & 1 & 1 & 1 & 1 \\
15 & . & . & 1 & . & . & 1 \\
16 & . & 1 & . & . & 1 & . \\
17 & 1 & . & . & 1 & . & . \\
18 & . & 1 & 1 & 1 & 1 & 1 \\
19 & 1 & 1 & 1 & 1 & 1 & . \\
20 & 1 & . & 1 & . & 1 & 1 \\
21 & . & . & . & . & . & 1
\end{array}$$

(62)[1]

Looking first for rows having the identity plus only one or other term, we see that $A^{15} = A^3 + I$; hence 3 and 15 are basic shifts. Next we look for rows that differ only in the identity (0) term. It is seen that $A^6 + I = A^9$; therefore 6 and 9 are basic shifts. Also, $A^7 + I = A^{14}$, so 7 and 14 are also basic shifts. Consequently,

$$\text{basic shifts} = \left\{3,\ 15;\ 6,\ 9;\ 7,14\right\} \tag{63}$$

By repeatedly doubling each one of these, the following list of permissible shifts is achieved:

$$\text{shifts} = \left\{3,\ 6,\ 12;\ 7,\ 14;\ 9,\ 18,\ 15\right\} \tag{64}$$

If we shift any given sequence an amount different from any of these numbers a sequence different from the original sequence will result. The above shifts,

[1] Dots have been used instead of zeros so that the patterning of ones is more evident.

then, describe the partial shift and add property of this non-maximal generator whose polynomial is irreducible.

Another important structure property that applies to a non-maximal generator with an irreducible polynomial is that there exists a matrix that relates all the sequences of the set. This property is very closely associated with the shift and add property discussed above. If we consider any shift that does not produce the same sequence then a matrix can be formed which commutes between the sequences of the set. That is, applying this matrix to one sequence of the set, another of the set results; if this is repeated for the resulting sequence, still another of the set results, etc. When all the sequences have been scanned the original sequence will result, but it may be shifted from the original one. If we call the various non-maximal sequences of the set u,v,w,etc., and label the commuting matrix as the "C" matrix, then

$$\begin{aligned} CU &= V \\ CV &= W \\ \vdots\ & \quad \vdots \\ CZ &= A^{x}U \end{aligned} \tag{65}$$

where u,v,w ---z = non-maximal length sequences resulting from a given SRG.

U = any n digits of the u sequence

V = any n digits of the v sequence

As mentioned above, a C matrix can be formed by using any of the shifts which do not give the same sequence with a shift. As an illustration, consider the generator [9,8,0] which was treated in equation (60); the shifts which exhibit the shift and add property are shown in equation (61). Hence, to form a C matrix we can use any shift (up to 73) not appearing in this equation. We will use the shift "3" to demonstrate a C matrix; thus we can write the equation:

$$(A^3 + I)U = V$$

$$C = A^3 + I \qquad (66)$$

where A = matrix for [9,8,0]

C = commuting matrix for the A generator

This equation says, that if we take any sequence of 'the set, shift it three times and then add this to the original, a different sequence of the set will be obtained. Furthermore different sequences of the set will be obtained by repeated applications of the C matrix as shown in equation (65). The generator [9,8,0] has a set of 7 sequences, each of length 73; the given C matrix then permutes between each of these seven sequences. Further, it is found that

$$C^7 = A^{61} \qquad (67)$$

This means that, when the C matrix is successively applied 7 times, so that all the sequences of the set have been scanned, the C matrix then returns to the original sequence, but shifted 61 digits from the original reference.

It should be noted that, in general, a C matrix formed as in equation (66) is not a companion matrix; of course, it will be similar to a companion matrix. Also it must be remembered that, in the above paragraphs, we were talking about generators with irreducible polynomials.

Having discussed the C matrix which relates the sequences from a non-maximal SSRG (with an irreducible polynomial), we are now led to an interesting property that relates this non-maximal SSRG to a set of maximal SSRG's of the same number of stages. In essence, all the sequences from a given irreducible SSRG (non-maximal) can be obtained by sampling the sequences from a set of maximal SSRG's. Although the sequences from the non-maximal generator can be achieved by some sampling of all the maximal generators of the same number of stages, we shall be most interested in those related maximal generators which yield the non-maximal sequences with a short sampling plan.

This relation between maximal and non-maximal generators is suggested when one considers the order of the commuting C matrix discussed above. If a C matrix permutes between all the sequences of a given non-maximal generator, then the C matrix must have a maximal order. Therefore if we consider a generator wired according to a given C matrix, that generator will be a maximal one. It is further suggested that a sampling of the sequence from this maximal generator will produce the sequences of the non-maximal one; this has been found to be true. It has been found that, if there are k equal-length sequences from a non-maximal generator, then by sampling every $k^{th}$ digit of the associated maximal generators, the sequences from the non-maximal one are obtained. If any sampling plan whatsoever is allowed, then the sequences from a non-maximal generator can be obtained from <u>any</u> maximal generator (of the same number of stages). There seems to be little point to this, however, and we shall consider as related only those maximal generators which can be sampled every $k^{th}$ digit to obtain the desired non-maximal sequences.

We will demonstrate the above principle by considering the C matrix of equation (66): $C = A^3 + I$. The A matrix refers to the [9,8,0] generator, and this SSRG has 7 sequences, each of length 73. The C matrix is not a companion matrix, and hence the generator for this would be a multiple-return one. Since every multiple-return generator has a simple equivalent, we seek the simple generator equivalent to the given C matrix. This can be accomplished by the same method used in Figure 8; 17 digits of the output sequence are needed. The generator [9,8,5,4,2,1,0] is the simple generator corresponding to the given C matrix, and experimentally it has been verified that this is a maximal generator. Now the set of 7 sequences from the non-maximal generator [9,8,0] are all of length 73. The above discussion stipulates that, by sampling the generator [9,8,5,4,2,1,0] every $7^{th}$ digit, we will obtain the sequences of [9,8,0.], and this has been found to be the case. Thus, we start anywhere in the maximal sequence and pick up every 7th digit; this is one of the non-maximal sequences of [9,8,0.] Then we move over one digit and repeat the selection, and another non-maximal sequence is obtained, etc.

Thus, we have found one 9-stage maximal generator which, if sampled every $7^{th}$ digit, produces the non-maximal sequences of [9,8,0.] The non-maximal generator possesses 7 equal-length sequences, and we have found a related maximal generator----related in the sense that every $7^{th}$ digit of the latters sequence forms the 7 sequences of the former. It was noted earlier that we can sample every 9-stage maximal generator and obtain the sequences of all the non-maximal ones (including [9,8,0] of course); however, this will require samplings other than every $7^{th}$ digit, and there seems to be little point in this. It is for this reason that we shall regard a maximal generator as related to a non-maximal one only if every $k^{th}$ digit of the former produces the k sequences of the latter.

In the above illustration we constructed the C matrix by knowing a proper "shift." We can, if we wish, synthesize a C matrix by using any two sequences of the set and any two reference points in these sequences.

If we formed the C matrix in such a manner, we would probably not know C in terms of A. Therefore the method of finding the simple generator corresponding to C that was used in Figure 8 would not be available. In this case it would be necessary to take advantage of the knowledge of the non-maximal sequences and their chosen references, and then construct the output sequence of the related maximal generator. Knowing this, it is possible to find the proper simple generator by the method of Figure 8 in Section 2.

It is now pertinent to consider how many maximal generators are related to a given non-maximal one in the manner stated above. The answer is as follows: if there are "r" non-maximal generators (for a given n stages) of a given length, and if there are "s" maximal generators of n stages, then there will be s/r maximal generators associated with each of the r generators in the above sense. Thus, for the 9-stage case there are 8 irreducible non-maximal generators (whose sequence lengths are all 73) and 48 maximal generators. Thus, with each non-maximal generator there are associated 6 maximal generators which, if sampled every 7th digit, produce the sequences of the given non-maximal one.

From Table II we find that, for the case of 8 stages, there are 16 maximal generators (L = 511), 8 non-maximal ones of length 85, 4 non-maximal ones of length 51, and 2 of length 17. Thus, for the 85 long SRG's, there will be 2 associated maximal generators which can be sampled every 3rd digit; there will be 4 maximal generators which can be sampled every 5th digit to produce the sequences of the 51 long generators; and 8 maximal SSRG's which can be sampled every 15th digit to find the sequences for any 17 long generator.

We will now demonstrate these conclusions by finding the 6 similarity classes for the maximal generators related to the [9,8,0] generator. In a preceding paragraph we found that one related maximal generator [9,8,5,4,2,1,0]. The similarity class for this connection is [1,2,4,8,16,32,64,128,256]. If we sample this connection every 7th, we are in effect reading the sequences of the similarity class [7,14,28,56,112,224,448,385,259]. Now, we want all the similarity classes which, if raised to the 7th power, give a number in this class (we shall chose the lowest number (7) for convenience). The essential procedure then is to find all those numbers which, modulo-511, equal 7; then this number is divided by 7, and the result establishes the correct similarity class. The following numbers are equal to 7, modulo-511

$$\begin{aligned} 7 &= 7\cdot 1 + (0)(511) &= 7 \pmod{511}\\ 7\cdot 74 &= 7\cdot 1 + (1)\ 511 &= 7 \pmod{511}\\ 7\cdot 147 &= 7\cdot 1 + (2)(511) &= 7 \pmod{511}\\ 7\cdot 220 &= 7\cdot 1 + (3)(511) &= 7 \pmod{511}\\ 7\cdot 293 &= 7\cdot 1 + (4)(511) &= 7 \pmod{511}\\ 7\cdot 366 &= 7\cdot 1 + (5)(511) &= 7 \pmod{511}\\ 7\cdot 439 &= 7\cdot 1 + (6)(511) &= 7 \pmod{511} \end{aligned} \tag{69}$$

It is clear that these are the only numbers which equal 7, modulo-511; the next number which would occur equals 1 (modulo-511) and hence the numbers would start to repeat. Note that the number 147 is divisible by 7, and hence this number will establish a similarity class which represents a non-maximal generator. For this reason we ignore it, since we are seeking those <u>maximal</u> generators which, if sampled every 7, given the sequences of [9,8,0]. Taking the remaining numbers then, to establish similarity classes we find the following classes:

$$\begin{aligned} &\{1,2,4,8,16,32,64,128,256\}\\ &\{74, 128,296,81,162,324,137,274,37\}\\ &\{220,440,369,227,454,397,283,55,110\}\\ &\{293,75,150,300,89,178,356,201,402\}\\ &\{366,221,442,373,235,470,429,347,183\}\\ &\{439,367,223,446,381,251,502,493,475\} \end{aligned} \tag{69}$$

These six classes now determine the six maximal generators which, if sampled every 7th digit, produce the sequences of the non-maximal generator [9,8,0].

Using the example of the [9,8,0] generator, then, we have just demonstrated that there are six maximal generators which are associated with this generator by means of a simple sampling plan. This is meant to serve as a demonstration of the above conclusions regarding the relation between non-maximal and maximal generators.

This concludes our consideration of the relationship between non-maximal generators and maximal ones when the generator's polynomial is irreducible. This gives us some idea of what happens when we sample a maximal SRG at a rate that is not relatively prime to its order. Earlier, in equation (27) we viewed the generation of maximal sequences as the sampling at relatively prime rates of one maximal sequence. Here we have seen that a sampling at a non-prime rate results in sequences which appear in a non-maximal SRG. This suggests more structure, which we did not pursue.

We have just seen that, when a non-maximal SRG has a polynomial that is irreducible, the resulting group of sequences are all of the same length and that this group of sequences exhibit some structure. Specifically, a matrix exists which relates all the sequences, one to the other, and that all the sequences in the group can be considered as being derived from a sampling a set of <u>maximal</u> SRG's which are related to the commuting matrix (C). All of this structure has been the result of investigating the shift and add properties of non-maximal sequences. We will find that a similar structure does not appear when the polynomial contains factors.

### 5.2.2 Non-Repeated-Factor Polynomials

Consider now the shift and add properties when the polynomial contains factors, but no factors are repeated. From the material considered in Section 5.1.2 (equations 49 through 54) it will be recalled that we must consider the cases where the p's are prime and non-prime and that within each of these the cases of maximal and non-maximal factors exist.

In general those shifts which produce the shift and add property are found in the manner identical to the case treated above (irreducible polynomial). If the p's are prime and the factors are maximal length ones (and only two feedbacks are present) the shifts which produce the shift and add property are found by grouping each term of the characteristic equation with the identity term, and then repeatedly squaring each of these terms. This results in a series of shifts, which, if applied to any sequence of the group, will result in obtaining a shifted version of the same sequence.

As an example of this type consider the equation (5,4,0) = (2,1,0) (3,1,0). It is noted that the orders of the factors are co-prime, and the factors represent maximal generators. From this equation the two basic shift properties are:

$$\begin{aligned} (A^4 + I)U &= A^5U \\ (A^5 + I)U &= A^4U \end{aligned} \qquad (70)$$

Hence the shifts of 4 and 5 are the two basic ones; using these and repeatedly squaring them (and using $A^{21} = I$), the following shifts are found to be permissible:

$$\left\{ 4,\ 8,\ 16,\ 11,\ 1,\ 2;\ 5,\ 10,\ 20,\ 19,\ 17,\ 13 \right\} \qquad (71)$$

The remaining shifts, if applied to a sequence of the group, will provide a different sequence when shifted and added.

If the p's are all relatively prime to each other and some or all of the factors are non-maximal ones the situation becomes more complex. First of all, the basic permissible shifts will still be determined by the characteristic equation as above. From any sequence of the group, these shifts will always return a shifted version of the same sequence. However, there will be another set of permissible shifts which operate within the non-maximal sequences of a given factor. That is, these shifts will be permissible only with the non-maximal sequences of the given factor.

If the p's are not prime their permissible shifts are still found in the same manner as above. The only essential difference is that a smaller number of shifts will be permissible. This is due to the fact that the order of the A matrix is reduced (from what is would be if all the factors' orders were prime); this means that the repeated squaring of the basic shifts is cut short. Hence a smaller number of permissible shifts will result.

Since we considered a commuting C matrix for the previous case of non-maximal generators with irreducible polynomials, it is natural to wonder whether a C matrix plays a similar role when the polynomials are factorable. In general it appears that there is less significance to a commuting matrix in this latter case. For one thing all the sequences in the group are not of the same length. Another general statement is that, if any of the factors are maximal ones any C matrix which commutes another sequence to that sequence cannot commute any further because the sequence of the maximal factor will have the complete shift and add property. Hence when maximal factors are present there cannot exist a C matrix which commutes between all the sequences of the group. In the case where the p's are not prime, it is possible to find a matrix that commutes between a part of the group of the sequences. An example of this is the generator whose equation is (8,1,0) = (2,1,0)(6,5,3,2,0). The orders 3 and 63 are not relatively prime. This generator provides 4 sequences that are 63 long, and one sequence of length 3. A C matrix can be found that permutes between 3 of the 4--63 long sequences (the 63 long sequence that is a maximal one is excluded).

In general, however, it appears that a C matrix does not add significantly to exhibiting structure behind non-maximal sequences when the polynomial is factorable.

### 5.2.3 Repeated Factor Polynomials

The last case we have to consider is when the polynomial has repeated factors. The situation here is similar to the case of non-repeated factors just treated. The permissible shifts are found from the characteristic equation or the $B_A$ matrix and a C matrix can only permute between parts of the total group of sequences. It has been observed that the permutation group is related to the power of the factor; if the power is two, a given C matrix permutes between two sequences at a time, etc.

Before concluding this section it is pertinent to mention those non-maximal sequences that can be obtained from generators with an odd number of feedback taps. It will be remembered that all the previous material was devoted to generators with an even number of taps. The reason for this restrictrion is that, as stated in Theorem 3, no SSRG with an odd number of taps can produce maximal sequences.

It will be shown that the set of non-maximal sequences from an odd feedback SSRG contains the same sequence as that from an even feedback generator of less stages plus a sequence or sequences related to this one. To show this we will utilize a theorem:

Theorem 8: If a modulo-two polynomial contains an even number of non-zero coefficients, it is divisible by the binomial (x + 1).

If the SSRG has an odd number of feedback taps its polynomial has an even number of terms (due to the added zero). The theorem than says: if an n stage SSRG has an odd number of taps, its polynomial can always be factored into $(x + 1)^r$ $(x^{n-r}$----------1). The second polynomial will always be of degree less than n; and it might also be factorable. Also, this second polynomial has an odd number of terms----hence the corresponding SSRG has an even number of taps.

Consider as an example the case where r = 1. Since the factor (1,0) corresponds to a one-stage SSRG, the above theorem results in the following: One sequence from this odd feedback SRG will be the sequence corresponding to the n-1 stage SRG whose polynomial is the second factor above; one sequence will be the complement of this sequence; and the final sequence will consist of the all one sequence. This conclusion is achieved from Theorem 7 and the fact that "supplementing" the feedback digit results in supplementing the output sequence----it is observed that adding constant one to whatever digit is fed back supplements this feedback digit. The above conclusion will be obvious if one considers the cascading of factors as illustrated previously in Figure 20.

It will be noted that the lengths of the sequences above add to $2^n-1$. Suppose we have an n stage register with odd feedback and with $r = 1$; then there are two sequences of length $2^{n-1}-1$, and one sequence of length 1. The total is:

$$(2^{n-1} - 1) + (2^{n-1} - 1) + 1 = 2^n - 1 = L \qquad (63)$$

Thus we see how the non-maximal sequences from an odd feedback generator are related, or reduced to, the non-maximal sequences that we have already considered. For r different that 1 other sequences, in addition to those described above, are obtained. If $r=2$ the complement of the second polynomials' sequence will also be obtained (the complement of a sequence is formed by changing every second digit of the original sequence).

We can now summarize the situation for non-maximal generators. In general one can determine the number and the lengths of the sequences by considering the characteristic polynomial of the generator. If the polynomial is irreducible the order of the matrix will specify the information; if the polynomial is factorable the information can be derived from the factors.

When considering the shift and add property we saw that non-maximal sequences have a "partial" shift and add property in that shifting and adding to get back the same sequence only works for certain shifts. For all three cases of polynomials the permissible shifts can be obtained from the characteristic equation of the SRG. Further we saw that the sequences from non-maximal SSRG's whose characteristic polynomial is irreducible exhibit a great deal of structure; i.e. there exists a C matrix which commutes between the entire group of sequences. This then leads to relating the original non-maximal SRG to a maximal SRG of the same number of stages. All of the sequences from the non-maximal generator can be obtained by time sampling the related maximal generator. Finally it was noted that those sequences from SSRG's whose characteristic polynomial is factorable do not exhibit this structure, and the C matrix appears to have little significance.

As a last point it was shown that the sequences from an odd feedback generator are included in those sequences obtainable from even feedback generators which have been considered throughout this report.

## Summary

The properties of maximal and non-maximal sequences from linear shift register generators have been studied with the use of the A matrix, which represents the generator, and its characteristic polynomial.

In dealing with maximal sequences in Section 4, it was shown that the number of sequences obtainable, for an n-stage generator, is $\frac{\phi(2^n-1)}{n}$. All of these output sequences will be of length $2^n - 1$. Two methods were described for finding the proper connections for these generators. The first method consists of first finding all the $n^{th}$ degree irreducible polynomials (which have an odd number of terms), and then eliminating the proper number of these which have periods less than $2^n - 1$. Each of the polynomials which remain correspond to a maximal generator. The second method allows one to identify all the maximal generators of n stages if one is known. In this method one first writes the different similarity classes, involving powers which are prime to $2^n - 1$, for the given generator. Then, using the $B_A$ matrix, a polynomial is associated with the lowest power of each of the similarity classes. The resulting polynomials are the characteristic polynomials for the desired maximal generators. Also, in Section 4, it was shown that every maximal sequence has the shift and add property and hence all maximal sequences have perfect autocorrelation functions.

For non-maximal sequences, Section 5, it was shown that for each given generator the number of sequences and their lengths can be determined by considering the factors of the characteristic polynomial. To accomplish this it is necessary to consider whether the impulse response lengths of the factors are relatively prime to each other, and whether the factors themselves represent maximal or non-maximal generators. In dealing with the shift and add properties of non-maximal sequences it was found that only some shifts result in obtaining the same sequence back again. A procedure was described for finding these permissible shifts.

Further, it was found that when the non-maximal generator has an irreducible characteristic polynomial the resulting sequences possess an important structure property in the form of a commuting C matrix. In this irreducible case a set of C matrices exist which will permute between all the sequences of the generator. The method for finding these C matrices was discussed. The set of C matrices were then considered as a set of maximal generators which are related to the original non-maximal one. The relation is that any of the C maximal generators can be sampled in a simple manner to obtain the sequences of the original non-maximal one. Thus, for the irreducible non-maximal generator, the set of C matrices establish a relation between the non-maximal one and a set of maximal generators. It was also concluded that, for non-maximal generators with reducible polynomials, the C matrices do not appear to play a very important part.

In conclusion it must be stressed that the sequences considered in this report are generated by linear shift register generators. There are two possibilities for accomplishing a non-linear generator: (1) using non-linear feedback, and (2) placing a non-linear output matrix on a linear generator.

The non-linear feedback generator would use both multiplication and modulo-two addition. If both of these are allowable it is possible to obtain all possible sequences of length $2^n - 1$ using only n-stage generators. Thus we can regard the $\frac{\phi(2^n-1)}{n}$ sequences of length $2^n - 1$ from linear maximal generators as a subset of the total possible sequences of this length which are obtainable from non-linear generators. Another property of non-linear generators is that the transients may be as long as $2^n - 2$, for an n-stage generator.

If a non-linear output is placed on the linear register all the transient and periodic properties of the linear register will be preserved. Therefore the transients will not be longer than n digits long. Also, with this arrangement it is possible to obtain all the possible sequences of the period of the linear generator. Thus if the linear generator is a maximal one, using a non-linear output enables one to obtain all the possible sequences that are $2^n - 1$ long.

# APPENDIX A

The easiest exposition of the text material does not follow the same order as the internal logic. For this reason the theorems of this appendix are not in the same order as they appear in the report. The ordering of this appendix is in accord with the internal logic but the numbering of the theorems coincides with the numbers in the text. All equation numbers are preceded by A; any equation number without the prefix A refers to the body of the report.

All the material in this first section A.1 will deal with SSRG's. The material in Section A.2 will deal wich general SRG's, and important equivalences between the general SRG and the SSRG's.

## A.1 Theorems dealing with SSRG's

The first set of items to be proved in this appendix deals with simple shift register generators (SSRG's), and the shift matrix A defined in Section 3.1. The general form of an A matrix for a 4-stage SSRG is the 4 x 4 matrix below

$$A = \begin{bmatrix} C_1 & C_2 & C_3 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \qquad \text{(A 1)}$$

The second, third, and fourth rows are the characterization of a simple shift-register generator, since the shift matrix will shift the contents of the first stage into the second, the second into the third, the third into the fourth--as simple as that, no modulo-two adders between stages. The term $a_{1,4} = 1$because the last stage must feed back to the first. The first lemma will show that the inverse of this matrix is simply

$$D = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & C_1 & C_2 & C_3 \end{bmatrix} \qquad \text{(A 2)}$$

because the product of these two is

$$D\ A \quad = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2C_1 & 2C_2 & 2C_3 & 1 \end{bmatrix} \qquad \text{(A 3)}$$

The elements of the matrix are from the field of integers modulo 2, and hence the terms

$$2C_i \equiv 0 \qquad (\text{mod } 2) \qquad \text{(A 4)}$$

The proof below is just a formalization of this procedure.

Lemma 1 If A is an SSRG, A has an inverse

Proof:

$$A = (a_{ij}) \qquad a_{1j} = c_j \qquad 1 \leq j \leq n$$

$$\text{where } c_n = 1 \qquad \text{(A 5)}$$

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

$$a_{i,j\neq i-1} = 0$$

$$\text{Consider } D = (d_{ij}) \qquad di,i+1 = 1 \qquad 1 \leq i \leq n-1$$

$$d_{i,j\neq i+1} = 0 \qquad \text{(A 6)}$$

$$d_{n,1} = 1$$

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

$$D\ A = (\sum_k d_{ik}\ a_{kj}) \qquad \text{(A 7)}$$

Now for $i < n$ only $d_{i,i+1} \neq 0$, and so the $\sum_k$ degenerates:

$$\sum_k d_{ik}\ a_{kj} = d_{i,i+1}\, a_{i+1,j} = 1 \text{ if } j=i$$

$$= 0 \text{ if } j\neq i \qquad \text{(A 8)}$$

For i=n

$$\sum_k d_{nk}\ a_{kj} = d_{n,1}\ a_{1,j} + \sum_{k=2}^{n} c_{k-1}\ a_{k,j} \qquad \text{(A 9)}$$

Because only $a_{j+1,j} \neq 0$ in the second sum, i.e. $k = j+1$

$$\begin{aligned}\sum_k d_{nk}\, a_{kj} &= 1\cdot c_j + c_j \quad 0 \quad (\mathrm{mod}\ 2)\ \ j \leq n\text{-}1 \\ &= 1\cdot c_j + 0 = 1 \qquad\qquad j = n\end{aligned} \qquad \text{(A 10)}$$

Hence D A = $(\delta_{ij})$ = I, proving that D in the inverse of A. (A 11)

In order to establish further basic properties of SSRG's we must recall the notation used in the report. The notation for the column vectors called contents or content vectors was introduced in Section 3, equation(5). Specifically,

$$u_i(j) = \text{contents of the } i^{th} \text{ cell after } j \text{ shifts}$$

and (5)

$$U(j) = (u_i(j))$$

When a SSRG is being used, the contents of cells simply shift down the register,

$$u_{i+1}\,(j+1) = u_i(j), \qquad o \leq i < n \qquad \text{(A 12)}$$

The limitation on the index is because the "physical" range of the cell index is from one to n. It is convenient in this appendix to ignore the physical meaning of the subscripts, and to allow the cell index to take on any value.

Since every SSRG has an inverse, the shift index is also allowed unlimited range without ambiguity. This is crystallized below.

Remark 1 For any given SSRG and given initial load Y(o), for all integers i, j, and k

$$y_i(j) = y_{i+k}\,(j+k). \qquad \text{(A 13)}$$

Another immediate consequence of the existence of an inverse for A is the existance of an "order" for A, and hence its periodic nature and the lack of transients. The next remark and two corollaries will establish this.

Remark 2 The null load $Y_o(0) = (y_i(o) = 0)$ has period one, i.e.

$$A\ Y_o(0) = Y_o(0) \tag{A 14}$$

because any sum of zeros is still zero.

As was mentioned throughout the body of the report, an output sequence is the successive contents of a given cell; for convenience, this is usually the last stage. This means that the null load will always yield the all-zero output sequence. In addition, a similar consequence is that n successive digits of an output sequence correspond to the contents of the register at some time during the production of those digits. For example, if the output is from the last stage, starting after the $j^{th}$ shift, Remark 1, leads to the relation:

$$(y_n(j),\ y_n(j+1), --- y_n(j+n-1)) = (y_n(j),\ y_{n-1}(j), --- y_1(j)) \overset{1-1}{\longleftrightarrow} Y(j) \quad \text{(A 15)}$$

In general

$$(y_k(j),\ y_k(j+1), --- y_k(j+n-1)) = (y_n(n-k+j), ..\ y_1(n-k+j)) \overset{1-1}{\longleftrightarrow} Y(n-k+j) \quad \text{(A 16)}$$

Because of these simple relations, the periodicity of an output sequence is equivalent to the periodic reappearance of the same register contents.

Corollary L 1.1

Using a SSRG, every initial content vector will reappear periodically. I.e. given A, $Y(o) \exists b$, a function of A & $Y(o) \ni A^bY(o) = Y(o)$.

Proof For the null load $Y_o(0)$, $b = 1$ can be used. (Remark 2)

For any specific non-null load $Y(o)$, consider the set of next $2^n$contents: $Y(o), Y(1), --- Y(2^n)$. Because there are only $2^n-1$ non-null vectors of zeros and ones, there is at least one repeated contents, say

$$Y(a) = Y(a+b) \tag{A 17}$$

That means that

$$A^aY(o) = A^{a+b}Y(o) \tag{A 18}$$

and applying the inverse a times

$$Y(o) = A^b \, Y(o). \qquad (A\ 19)$$

and apply the shift k times

$$Y(k) = A^b \, Y(k) \qquad (A\ 20)$$

Corollary L 1.2

The shift matrix of a SSRG has an order, and the order is the least common multiple of the periods associated with the different possible initial loads.

Proof The Corollary L 1.1 proved that each initial contents will reappear periodically. The period of a periodic event is the minimum such periodicity. Since there are a finite number of initial conditions, there are only a finite number of such periods, and hence there will be a least common multiple. Call this l.c.m. b*. Since b* is a multiple of every period,

$$Y(o) = A^{b*} \, Y(o) \qquad (A\ 21)$$

for all vectors Y(o), then

$$I = A^{b*} \qquad (A\ 22)$$

Finally, assume there is some lower power of A which equals the identity, then equation (A 21) holds for this lower power is a common multiple of all periods, and this contradicts the definition of $b^*$ as the least common multiple.

Now that it has been established that all possible output sequences from a SSRG are periodic with no "transient" section, there will be no error involved in using the "obvious" definition that two sequences are the same if translating one in time will align it with the other so that there is complete agreement, digit by digit for one full period. Two sequences are different if there is no such translation possible.

Theorem 1. For a given n-stage SSRG, each possible n-tuple of zeros and ones appears in one and only one sequence.

Proof Given any n-tuple of digits $(d_1, d_2, \text{---} d_n)$, there is the possible initial load

$$Y(o): y_i(o) = d_{n+1-i} \qquad \text{(A 23)}$$

Consider the output sequence $y_n(j)$ for small j

$$y_n(j) = y_{n-j}(o) = d_{n+1-(n-j)} \qquad \text{(A 24)}$$

$$= d_{j+1}, \; o \leq j \leq n-1$$

That is, the specified n-tuple appears in the sequence corresponding to a content vector (initial or shifted) with those specified digits reading from bottom to top.

To show that these digits are in only one sequence, suppose two sequences contain the digits $d_1$ to $d_n$; consider the contents vector of equation (A 23). This must have been the contents of the SSRG at the time the digit $d_1$ was produced, and hence both sequences are the same as the sequence $y_n(j)$, where Y(o) is given by (A 23).

In the body of this report, the period of the impulse response $(Y(o) = (\delta_{i1})$, a simple one in the first stage) is denoted by $\ell$, and the periods of the other non-null sequences are denoted by p, $p_2$, etc. Considering a specific n-tuple in a sequence from an n-stage SSRG, this n-tuple reappears periodically with exactly the period of that sequence. Thus in the impulse response sequence there are $\ell$ different n-tuples which reappear in the same order.

Corollary 1.1 Considering all of the different sequences of a specific SSRG, then

$$\ell + \Sigma \, p_i = L \qquad (3)$$

Proof $L = 2^n - 1$ = number of non-null n-tuples.

The objective of the next two lemmas is to reach theorem 2, "the period of every sequence from a SSRG divides the impulse response period $\ell$." For this proof we need one more item of notation for special content vectors. These special vectors are the "elementary loads" consisting of a single one in some stage. A subscripted E for "elementary" is used instead of the usual "Y".

DEFINITION The $j^{th}$ elementary load is the vector

$$E_j(0) = (\delta_{i,j}) \tag{A 25}$$

As in the ordinary use of the notation, if an SRG A is being used, then the $k^{th}$ contents after an elementary load is

$$A^k E_j(0) = E_j(k)$$

Lastly, the sequence which results from the elementary load $E_j(0)$ is denoted as the sequence $E_j$.

LEMMA 2 The period of any sequence from a given SSRG divides the least common multiple of the periods of the elementary sequences.

Proof Consider any initial load

$$Y(0) = (y_i(0)). \tag{A 26}$$

In terms of the elementary loads

$$Y(0) = \sum_{i=1}^{n} y_i(0) E_i(0) \tag{A 27}$$

since each $E_i(0)$ contains exactly one 1 in the appropriate row.

Applying the shift matrix A to the sum of (A 27) we have

$$\begin{aligned} Y(k) = A^k Y(0) &\equiv \sum_{i=1}^{n} y_i(0) A^k E_i(0) \pmod 2 \\ &\equiv \sum_{i=1}^{n} y_i(0) E_i(k) \pmod 2 \end{aligned} \tag{A 28}$$

Reading equation (A 28) for the contents of any particular stage: "The initial load Y(0) selects which elementary sequences are to be added together to form the output sequence." Since the sum of periodic sequences is periodic, with period equal to or dividing the least common multiple of the periods of the summed sequences, the lemma is proved.

The impulse response is the sequence $E_1$. Since no special use is made of the actual digits of the impulse response elsewhere in the report, no general notation is established for it. However, from here to the end of the proof of Lemma 4, an asterisk will be used to denote the impulse response sequence.

$$Y^*(j) = E_1(j)$$

and (A 29)

$$\text{IR sequence: } y_n{}^*(j)$$

Note that for a SSRG,

$$\begin{aligned} y_n^*(j) &= y_{n-j}^*(0) = 0 \qquad 0 \le j \le n-2 \\ y_n^*(n-1) &= y_1^* \ (0) = 1 \end{aligned} \qquad \text{(A 30)}$$

It will be very useful to consider the matrix whose columns are the first n content vectors of the register with the impulse load. Hence the following definition:

<u>DEFINITION</u> The matrix $E_A$ associated with a SSRG A is defined as

$$E_A = (E_1(0),\ E_1(1),\ .\ .\ .\ E_1(n-1)) \qquad \text{(A 31)}$$

The elements of the matrix $E_A$ are related to the digits of the impulse response. Specifically, the elements in the $i^{th}$ row and $j^{th}$ column, usually denoted $e_{ij}$, is the $i^{th}$ cell contents after j-1 shifts

$$e_{ij} = y_i^*(j-1) = y_n^*(n+j-i-1) \qquad \text{(A 32)}$$

In particular it can be seen from equation (A 30) that the principal diagonal is all ones,

$$e_{i,i} = y_n^*(n+i-i-1) = y_n^*(n-1) = 1; \qquad \text{(A 33a)}$$

and the subdiagonal triangle is all zeros,

$$e_{i > j} = y_n^* (n-1-(i-j)) = 0. \qquad \text{(A 33b)}$$

LEMMA 3 The elementary loads are linear combinations of the first n impulse response contents $E_1(0), \ldots, E_1(n-1)$.

Proof Because $E_A$ is triangular, the determinate of $E_A$ is the product of the elements on the principal diagonal.

$$|E_A| = \prod_{j=1}^{n} e_{jj} = 1 \qquad \text{(A 34)}$$

Because the determinate is non-zero, the matrix has an inverse, $E_A^{-1}$.

$$E_A\, E_A^{-1} = I \qquad \text{A 35)}$$

Now the columns of $E_A$ are the first n content vectors under the initial load $E_1(0)$, while the columns of the identity I are the elementary loads $E_j(0)$. Thus the existance of the inverse, and its definition (A 35) becomes

$$(E_1(0), E_1(1), \ldots, E_1(n-1)\ ) \cdot E_A^{-1} \equiv (E_1(0), \ldots, E_n(0)\ ) \pmod 2 \quad \text{(A 3}$$

Thus the rows of $E_A^{-1}$ specify the desired linear combinations of coefficients which express the elementary loads as combinations of the first n impulse response contents. Using the above two lemmas, Theorem 2 can now be proved.

Theorem 2 The period of any sequence from a SSRG divides the impulse response period, i.e., $p_i | \ell$.

Proof By lemma 3, each elementary load is a linear combination of the first n content vectors under the impulse load. Hence each elementary sequence is a sum of shifted versions of the impulse response sequence. The resulting sum will be periodic every $\ell$ digits since it is a sum of sequences with period $\ell$. Because $\ell$ is the period of the first elementary load, $\ell$ is the least common multiple of the periods of the elementary sequences. The theorem then follows directly from Lemma 2.

Corollary 2.1 The order of a SSRG is the period of its impulse response.

Proof By Theorem 2, and the fact that SSRG's have no transient response,

$$A^{\ell}Y(0) \equiv Y(0) \qquad (\text{mod } 2) \qquad\qquad (A\ 37)$$

Further

$$A^{k}E_1(0) \not\equiv E_1(0) \qquad (\text{mod } 2) \quad 0 < k < \ell \qquad\qquad (A\ 38)$$

by definition of $\ell$. Since equation (A 37) holds for all Y(0), $\ell$ is the least power of A which is equal to the identity.

Although the material in the remainder of this section has no direct relation to the material in the report, it is deemed of sufficient importance to warrant its insertion here. This material deals with the fact that it can be very useful to know the relation between the elementary loads and the impulse response more specifically than as the inverse of the $E_A$ matrix. It will now be shown that this inverse is simpler to obtain than $E_A$, and that it is the feedback matrix $F_A$ defined below.

DEFINITION For a SSRG having the feedback

$$A: \ y_0(j) \equiv \sum_{k=1}^{n} c_k y_k(j) \quad (\text{mod } 2) \qquad\qquad (A\ 39)$$

the associated feedback matrix $F_A$ is the triangular matrix

$$\begin{aligned} f_{i,j} &= c_{j-i} & i < j \\ &= 1 & i = j \\ &= 0 & i > j \end{aligned} \qquad\qquad (A\ 40)$$

LEMMA 4 $F_A$ is the inverse of the elementary matrix $E_A$, i.e., $F_A E_A = I$.

Proof Form the product $P = F_A E_A$

$$p_{ij} \equiv \sum_{k=1}^{n} f_{ik}\ e_{kj} \ (\text{mod } 2) \qquad\qquad (A\ 41)$$

By definitions of $E_A$ and $F_A$, equations (A 32) and (A 40),

$$p_{ij} \equiv \sum_{k=i}^{n} c_{k-i}\, y_n^* \,(n+j-k-1), \pmod 2 \qquad \text{(A 42)}$$

where

$$c_o = 1$$

is added for simplicity.

Shifting the index on the summation

$$p_{ij} \equiv \sum_{r=o}^{n-i} c_r\, y_n{}^* \,(n+j-r-i-1) \pmod 2 \qquad \text{(A 43)}$$

or

$$p_{ij} \equiv \sum_{r=o}^{n-i} c_r\, y_r^* \,(j-i-1) \qquad \pmod 2 \qquad \text{(A 44)}$$

Three cases are considered depending on the magnitudes of i and j. For $i > j$ (the subdiagonal triangle of the product) the argument of $y_n^*$ in (A 43) is bounded between zero and n-2, which is shown as follows:

$$n - i \geq \quad r \quad \geq 0 \qquad \text{(A 45)}$$

$$n+j-(n-i)-i-1 \leq n+j-r-i-1 \leq n+j-i-1 \qquad \text{(A 46)}$$

The left hand side of (A 46) is j-1, which is non-negative, and the right hand side of (A 46) can be grouped as

$$n+j-i-1 = n-1-(i-j) \leq n-2. \qquad \text{(A 47)}$$

For this range of argument, the impulse response digits are zero (see equation A 30). Hence

$$p_{i\,>\,j} = 0 \qquad \text{(A 48)}$$

The second case is i=j

$$p_{ii} \equiv \sum_{r=o}^{n-i} c_r\, y_n(n-r-1) \qquad \pmod 2$$

$$p_{ii} \equiv c_o y_n(n-1) + \sum_{r=1}^{n-i} c_r y_n\,(n-r-1) \pmod 2 \qquad \text{(A 49)}$$

This last summation is zero, since the arguments range from n-2 down to i-1. By equation (A 42), $c_o$ is one, and by (A 30), $y_n^*(n-1)$ is one. Thus

$$p_{ii} = 1 \qquad \text{(A 50)}$$

For i < j the summation is not so trival, and must be further manipulated. The first trick is to notice that

$$y^*_r\ (j-i-1) = y^*_n\ (n-r+j-i-1) \qquad \text{(A 51)}$$

and for

$$n \geq \quad r \quad \geq n-i+1 \qquad \text{(A 52)}$$

$$0 \leq j-i-1 \leq n-r+j-i\ -1 \leq n-(n-i+1)+j-i-1 = j-2$$

Since this is the range for which $y^*_n$ is zero,

$$\sum_{r=n-i+1}^{n} c_r\ y^*_r\ (j-i-1) \equiv 0 \qquad \text{(mod 2)} \qquad \text{(A 53)}$$

Adding this zero to equation (A 44)

$$p_{ij} \equiv \sum_{r=o}^{n} c_r y^*_r\ (j-i-1). \quad \text{(mod 2)} \qquad \text{(A 54)}$$

The feedback equation, equation (A 39) can be rewritten as

$$0 \equiv \sum_{k=o}^{n} c_k\ y_k\ (j) \quad \text{(mod 2)} \qquad \text{(A 55)}$$

Since the impulse response sequence y* is generated according to this feedback law, (A 55) holds for y*, and comparison with (A 54) yields

$$p_{i\,<\,j} = 0 \qquad \text{(A 56)}$$

Collecting (A 48), (A 50), and (A 56) we have the result that P = I and hence $F_A$ is the inverse of the elementary matrix $E_A$.

## A·2 Theorems dealing with SRG's

The theorems in Section A 1 dealt specifically with SSRG's. In this section those properties which are true for general SRG's are considered, and the conditions under which the general SRG has an equivalent

SSRG is treated. The main features of a SSRG which distinguish it from a general SRG are the guaranteed existence of an inverse, and the index manipulation which relates output sequences to register contents, equation (5).

Certain properties of an SRG can be easily established from those of the SSRG. For instance, Remark 2 "The period of the null sequence is 1" is still obviously true. Since Corollaries L 1.1 and L 1.2 followed from the existence of an inverse, we can conclude the following remark.

Remark 3 If an SRG has an inverse, there will be no transient segments to the output sequences, and the A matrix for the SRG has an order equal to the l.c.m. of the periods of the different output sequences.

DEFINITION: A sequence law corresponds to an algebraic equation as follows

$$\sum_{i=o}^{n} c_i \, \xi^i \equiv 0 \quad \xleftrightarrow{1-1} \sum_{i=o}^{m} c_i u(i+k) \equiv 0 \quad (\text{mod } 2) \quad o \leq k \qquad (A\ 57)$$

LEMMA 5: The sequence of contents of each cell of a shift register obey each sequence law that corresponds to an equation that the shift matrix satisfies.

Proof

Assume A satisfies $\sum_{j=o}^{m} d_j \, \xi^j \equiv 0$ (mod 2) that is

$$\sum_{j=o}^{m} d_j \, A^j Y(k) \equiv 0 \ (\text{mod } 2) \text{ for all contents } Y(k) \qquad (A\ 58)$$

Thus

$$\sum_{j=o}^{m} d_j \, Y(j+k) \equiv 0 \quad (\text{mod } 2) \qquad o \leq k \qquad (A\ 59)$$

Because Y is a column vector $(y_i)$, (A 59) must be simultaneously satisfied by each row of Y;

$$\sum_{j=o}^{m} d_j y_i \ (j+k) \equiv 0 \pmod 2 \qquad o \leq k \qquad \text{Q.E.D.} \qquad (A\ 60)$$

If we single out the sequence law that corresponds to the characteristic equation, and call it the characteristic sequence law, the a natural consequence of Lemma 5 is Theorem 8.

Theorem 8 The sequence of cell contents of each stage of a SRG obeys the characteristic sequence law.

LEMMA 6 Any finite shift-and-sum of the digits of a sequence obeys every sequence law that the original sequence obeys.

Proof: Let the original sequence u obey the sequence law

$$0 \equiv \sum_{i=o}^{m} c_i \ u(k+i) \pmod 2 \qquad (A\ 61)$$

and the new sequence is the sum of u delayed $S_1$, $S_2$, --- up to $S_k$ shifts.

$$Z(j) \equiv \sum_{r=1}^{k} u(j+S_r) \pmod 2 \qquad (A\ 62)$$

Then the trial sum

$$\sum_{i=o}^{m} c_i \ Z(j+i) \equiv \sum_{i=o}^{m} c_i \sum_{r=1}^{k} u(j+i+Sr) \pmod 2$$

$$\equiv \sum_{r=1}^{k} \sum_{i=o}^{m} c_i u(j+S_r+i) \pmod 2 \qquad (A\ 63)$$

$$\sum_{r=1}^{k} 0 \equiv 0 \pmod 2 \quad \text{Q.E.D.}$$

The following material treats the equivalent simple shift register, for those SRG's that have simple equivalents. The objective is to show that the simple equivalent generates all of the sequences of the SRG; it may generate some additional ones too. In the same vein a simplified generator called the characteristic shift register generator, CSRG, is introduced to play the same role for all SRG's, not just those with simple equivalents. If the SRG has a simple equivalent, that simple equivalent and the CSRG are the same. If the SRG has no simple equivalent, the CSRG consists of a short SRG feeding some additional delay stages.

<u>DEFINITION</u>: The matrix, $S_A$, of the CSRG associated with a shift matrix A is the rotate of the companion matrix of the characteristic equation of A. In symbols, if

$$|A + \xi\ I| \equiv \xi_n + c_1\ \xi^{n-1} + \text{---}\ c_n\xi^o \pmod{2} \qquad \text{(A 64)}$$

then

$$S_A = (s_{ij}) \ni s1j = c_j \qquad i = 1 \qquad \text{(A 65)}$$

$$\text{and } s_{ij} = \delta_{i,j-1} \quad 2 \leq i \leq n$$

<u>Cor</u> $|A+\xi I| \equiv |S_A + \xi I| \pmod{2}$ (A 66)

<u>Cor</u> If A is an SSRG, $A = S_A$.

<u>Cor</u> $S_A$ is a SSRG if and only if $c_n$=1 in equation (A 64)

<u>Cor</u> $S_A$ is non-singular if and only if $S_A$ is a SSRG

Theorem 1 for SSRG's states that each n-tuple appears in some sequence from the SSRG. Since by Theorem 8 all sequences obey the characteristic sequence law, which relates each digit to no more than n preceding digits, all sequences that obey that law are produced by the SSRG.

<u>Remark 4</u>: If an SRG has an SSRG as a characteristic shift matrix, the sequences of the SRG (as well as those formed by shifted sums of these) will be among those of the SSRG. These sequences have no transient sections.

This remark substantiates the statement made in the report: if the characteristic equation has a non-zero constant term then the SRG has an equivalent SSRG.

Remark 5: A CSRG enjoys almost the same index manipulation as a SSRG, (Remark 1), namely

$$y_i(j) = y_{i+k}(j+k) \qquad \text{for all } i; \text{ and for } j,\ k \geq 0 \qquad \text{(A 67)}$$

The shift indices are restricted to the positive range because of the possible lack of an inverse.

If the proof of Theorem 1 is reviewed it is seen that it is an immediate consequence of the index manipulation. Hence we can make an equivalent statement for CSRG's.

Remark 6. For a given n-stage CSRG each possible n-tuple of zeros and ones appears in one and only one sequence. Part of this n-tuple may be in the transient section of the sequence.

Combine this with Theorem 8 the same way as Theorem 1 was above in Remark 4--namely, that the appearance of every n-tuple in some sequence together with an $n^{th}$ degree characteristic equation means that cell sequences obeying the characteristic are generated by the CSRG.

Remark 7. The sequences of an SRG, and the sequences formed by summing shifted versions of these sequences, are among the sequences produced by the corresponding CSRG.

Finally we consider the transient of the sequence. If the CSRG matrix's first row is given by

$$\begin{aligned} s_{1,j} &= c_j \qquad j = 1,2,\text{---}k\text{-}1 \qquad \text{(A 68)} \\ s_{1,k} &= 1 \\ s_{1,j} &= 0 \qquad j = k+1,\ \text{---}n \end{aligned}$$

the generator is a k-stage SSRG followed by n-k stages with no feedback connections. Obviously the transient is no more than (n-k) digits long, followed by the periodic sequences possible from the corresponding k-stage SSRG. This is a complete characterization; only one feature is specifically singled out.

Remark 8. The transient of an n-stage SRG occupies no more than n digits.

## Section A.3: Characteristic Equations of SSRG's

These last few theorems of the appendix deal with the characteristic polynomials of SSRG's and their factors. The characteristic polynomial of an SSRG has a non-zero term.

Theorem 7 If the characteristic polynomial of an SSRG is factorable, consider the sequences that are generated by the SSRG's which have these factors as characteristics. These are also generated by the given SSRG.

Proof Every factor of the characteristic polynomial has a non-zero constant term (because the product does), and hence is the characteristic of some SSRG. Consider the factor $f(\xi)$ of the characteristic polynomial $p(\xi)$

$$p(\xi) \equiv q(\xi)\, f(\xi) \qquad (\text{mod } 2) \qquad (\text{A } 69)$$

Let
$$p(\xi) = \sum_{i=o}^{n} p_i \xi^i \qquad (\text{A } 70)$$

$$f(\xi) = \sum_{k=o}^{m} f_k \xi^k$$

and

$$q(\xi) = \sum_{s=o}^{n-m} q_s \xi^s$$

where the $p_i$ are related by the usual product formulae

$$p_i \equiv \sum_{r=o}^{i} q_{i-r}\, fr \qquad (\text{mod } 2) \qquad (\text{A } 71)$$

Any sequence $y(j)$ generated by the SSRG with characteristic polynomial $f(\xi)$ obeys the corresponding characteristic sequence law:

$$\sum_{k=o}^{m} f_k y(k+j) \equiv 0 \quad (\text{mod } 2) \text{ for all } j \tag{A 72}$$

Hence the sum of n-m of these is still zero

$$\sum_{s=o}^{n-m} q_s \left( \sum_{k=o}^{m} f_k \, y(k+j+s) \right) \equiv 0 \quad (\text{mod } 2) \tag{A 73}$$

Collect terms

$$\sum_{s=o}^{n-m} \sum_{k=o}^{m} q_s f_k \, y(k+j+s) \equiv 0 \quad (\text{mod } 2) \tag{A 74}$$

and use the index change s=i-k, to obtain

$$\sum_{i=o}^{n} \sum_{k=o}^{i} q_{i-k} f_k y(i+j) \equiv 0 \quad (\text{mod } 2) \tag{A 75}$$

The coefficient of y(i+j) is simply $p_i$ by (A 71)

$$\sum_{i=o}^{n} p_i y(i+j) \equiv 0. \quad (\text{mod } 2) \tag{A 76}$$

That is, the sequence obeys the characteristic sequence law associated with p(ξ). By Remark 6, this sequence will be one of the sequences from the SSRG with the characteristic polynomial p(ξ).

Q.E.D

An immediate corollary is Theorem 5.

Theorem 5 No SSRG with a factorable characteristic polynomial is maximal.

Theorem 8 Every polynomial with an even number of non-zero coefficients is divisable by (ξ+1) i.e., by (1,0).

Proof If $p(\xi) = \sum_{i=o}^{n} p_i \xi^i$ has an even number of coefficients, then the sum of the coefficients is even:

$$\sum_{i=o}^{n} p_i \equiv 0 \quad (\text{mod } 2) \tag{A 77}$$

Hence

$$p(I) = \sum_{i=o}^{n} p_i I^i = (\sum_{i=o}^{n} p_i) \, I \equiv 0 \quad (\text{mod } 2) \tag{A 78}$$

Because the identity is a root of $p(\xi)$, the minimum polynomial of the identity divides $p(\xi)$. This minimum polynomial is $\xi+1$. Q.E.D.

Cor Every SSRG with an even number of non-zero coefficients will produce the all-one sequence.

Proof The all-one sequence obeys the sequence law

$$y(j+1) + y(j) \equiv 0 \qquad (\text{mod } 2) \qquad (\text{A } 79)$$

which corresponds to the polynomial $(\xi+1)$.

Another corollary is Theorem 3.

Theorem 3 Every SSRG with an odd number of feedback taps is non-maximal.

Proof An odd number of taps implies an even number of non-zero coefficients in the characteristic polynomial. Now apply Theorems 9 and 5.

# APPENDIX B

In Section 4.2.2 of the report, the second method for determining all maximal connections from the characteristic equation and $B_A$ matrix of one maximal connection was discussed. The example used there was the derivation of all eight stage maximal SSRG's from the one with characteristic polynomial (8,7,2,1,0). Figure 17a shows the $B_A$ matrix up through the fifty-second row,while Figure 17b shows the derivation of the characteristic polynomial for the similarity class containing $A^7$, and Figure 17c shows the work for $A^{11}$. The remaining similarity classes are given in equation (38) and the lowest powers of those classes are 13, 19, 23, 37, and 43. The characteristic equations for the other eight classes are found by reversing the characteristic equations derived for these classes. For example, equation (38) lists the similiarity class beginning with $A^{127}$ as being the reverse of that beginning with $A^1$; $A^1$ has the feedback [8,7,6,1,0] and therefore $A^{127}$ has characteristic polynomial (8,7,6,1,0).

Rows fifty-seven through one hundred eighty-seven of the $B_A$ matrix are given below. Using this and Figure 17a, all of the necessary equations are listed except those for rows 215 and 222. These were easily picked up from the low part of the table as follows: From row 107 one obtains the polynomial (107,3,2,1). Squaring this yields (214,6,4,2). Multiply by A to form (215,7,5,3), the desired row. From row 111 one obtains the polynomial (111,7,6,5) which squares to (222,14,12,10). This is reduced by using rows 14,12, and 10 to form (222, 5, 4, 1).

| n | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| 57 | . | 1 | 1 | 1 | 1 | 1 | 1 | . |
|  | 1 | 1 | 1 | 1 | 1 | 1 | . | . |
|  | . | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 60 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . |
|  | . | 1 | 1 | 1 | 1 | . | 1 | 1 |
|  | 1 | 1 | 1 | 1 | . | 1 | 1 | . |
|  | . | 1 | 1 | . | 1 | . | 1 | 1 |
|  | 1 | 1 | . | 1 | . | 1 | 1 | . |
|  | . | . | 1 | . | 1 | . | 1 | 1 |
|  | . | 1 | . | 1 | . | 1 | 1 | . |
|  | 1 | . | 1 | . | 1 | 1 | . | . |
|  | 1 | 1 | . | 1 | 1 | 1 | 1 | 1 |
|  | . | . | 1 | 1 | 1 | . | . | 1 |
| 70 | . | 1 | 1 | 1 | . | . | 1 | . |
|  | 1 | 1 | 1 | . | . | 1 | . | . |
|  | . | 1 | . | . | 1 | 1 | 1 | 1 |
|  | 1 | . | . | 1 | 1 | 1 | 1 | . |
|  | 1 | . | 1 | 1 | 1 | . | 1 | 1 |
|  | 1 | 1 | 1 | 1 | . | . | . | 1 |
|  | . | 1 | 1 | . | . | 1 | . | 1 |
|  | 1 | 1 | . | . | 1 | . | 1 | . |
|  | . | . | . | 1 | . | . | 1 | 1 |
|  | . | . | 1 | . | . | 1 | 1 | . |
| 80 | . | 1 | . | . | 1 | 1 | . | . |
|  | 1 | . | . | 1 | 1 | . | . | . |
|  | 1 | . | 1 | 1 | . | 1 | 1 | 1 |
|  | 1 | 1 | 1 | . | 1 | . | . | 1 |
|  | . | 1 | . | 1 | . | 1 | . | 1 |
|  | 1 | . | 1 | . | 1 | . | 1 | . |
|  | 1 | 1 | . | 1 | . | . | 1 | 1 |
|  | . | . | 1 | . | . | . | . | 1 |
| 88 | . | 1 | . | . | . | . | 1 | . |
|  | 1 | . | . | . | . | 1 | . | . |
| 90 | 1 | . | . | . | 1 | 1 | 1 | 1 |
|  | 1 | . | . | 1 | 1 | . | . | 1 |
|  | 1 | . | 1 | 1 | . | 1 | . | 1 |
|  | 1 | 1 | 1 | . | 1 | 1 | . | 1 |
|  | . | 1 | . | 1 | 1 | 1 | . | 1 |
|  | 1 | . | 1 | 1 | 1 | . | 1 | . |
|  | 1 | 1 | 1 | 1 | . | . | 1 | 1 |
|  | . | 1 | 1 | . | . | . | . | 1 |
|  | 1 | 1 | . | . | . | . | 1 | . |
|  | . | . | . | . | . | . | 1 | 1 |
| 100 | . | . | . | . | . | 1 | 1 | . |
|  | . | . | . | . | 1 | 1 | . | . |
| 101 | . | . | . | . | 1 | 1 | . | . |
|  | . | . | . | 1 | 1 | . | . | . |
|  | . | . | 1 | 1 | . | . | . | . |
|  | . | 1 | 1 | . | . | . | . | . |
|  | 1 | 1 | . | . | . | . | . | . |
|  | . | . | . | . | . | 1 | 1 | 1 |
|  | . | . | . | . | 1 | 1 | 1 | . |
|  | . | . | . | 1 | 1 | 1 | . | . |
|  | . | . | 1 | 1 | 1 | . | . | . |
| 110 | . | 1 | 1 | 1 | . | . | . | . |
|  | 1 | 1 | 1 | . | . | . | . | . |
|  | . | 1 | . | . | . | 1 | 1 | 1 |
|  | 1 | . | . | . | 1 | 1 | 1 | . |
|  | 1 | . | . | 1 | 1 | . | 1 | 1 |
|  | 1 | . | 1 | 1 | . | . | . | 1 |
|  | 1 | 1 | 1 | . | . | 1 | . | 1 |
|  | . | 1 | . | . | 1 | 1 | . | 1 |
|  | 1 | . | . | 1 | 1 | . | 1 | . |
|  | 1 | . | 1 | 1 | . | . | 1 | 1 |
| 120 | 1 | 1 | 1 | . | . | . | . | 1 |
|  | . | 1 | . | . | . | 1 | . | 1 |
|  | 1 | . | . | . | 1 | . | 1 | . |
|  | 1 | . | . | 1 | . | . | 1 | 1 |
|  | 1 | . | 1 | . | . | . | . | 1 |
|  | 1 | 1 | . | . | . | 1 | . | 1 |
|  | . | . | . | . | 1 | 1 | . | 1 |
|  | . | . | . | 1 | 1 | . | 1 | . |
|  | . | . | 1 | 1 | . | 1 | . | . |
|  | . | 1 | 1 | . | 1 | . | . | . |
| 130 | 1 | 1 | . | 1 | . | . | . | . |
|  | . | . | 1 | . | . | 1 | 1 | 1 |
|  | . | 1 | . | . | 1 | 1 | 1 | . |
|  | 1 | . | . | 1 | 1 | 1 | . | . |
|  | 1 | . | 1 | 1 | 1 | 1 | 1 | 1 |
|  | 1 | 1 | 1 | 1 | 1 | . | . | 1 |
|  | . | 1 | 1 | 1 | . | 1 | . | 1 |
|  | 1 | 1 | 1 | . | 1 | . | 1 | . |
|  | . | 1 | . | 1 | . | . | 1 | 1 |
|  | 1 | . | 1 | . | . | 1 | 1 | . |
| 140 | 1 | 1 | . | . | 1 | . | 1 | 1 |
|  | . | . | . | 1 | . | . | . | 1 |
|  | . | . | 1 | . | . | . | 1 | . |
|  | . | 1 | . | . | . | 1 | . | . |
|  | 1 | . | . | . | 1 | . | . | . |
|  | 1 | . | . | 1 | . | 1 | 1 | 1 |
|  | 1 | . | 1 | . | 1 | . | . | 1 |
|  | 1 | 1 | . | 1 | . | 1 | . | 1 |
|  | . | . | 1 | . | 1 | 1 | . | 1 |
|  | . | 1 | . | 1 | 1 | . | 1 | . |
| 150 | 1 | . | 1 | 1 | . | 1 | . | . |
| 151 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 |
|  | . | 1 | . | 1 | 1 | . | . | 1 |
|  | 1 | . | 1 | 1 | . | . | 1 | . |
|  | 1 | 1 | 1 | . | . | . | 1 | 1 |
|  | . | 1 | . | . | . | . | . | 1 |
|  | 1 | . | . | . | . | . | 1 | . |
|  | 1 | . | . | . | . | . | 1 | 1 |
|  | 1 | . | . | . | . | . | . | 1 |
|  | 1 | . | . | . | . | 1 | . | 1 |
| 160 | 1 | . | . | . | 1 | 1 | . | 1 |
|  | 1 | . | . | 1 | 1 | 1 | . | 1 |
|  | 1 | . | 1 | 1 | 1 | 1 | . | 1 |
|  | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 |
|  | . | 1 | 1 | 1 | 1 | 1 | . | 1 |
|  | 1 | 1 | 1 | 1 | 1 | . | 1 | . |
|  | . | 1 | 1 | 1 | . | . | 1 | 1 |
|  | 1 | 1 | 1 | . | . | 1 | 1 | . |
|  | . | 1 | . | . | 1 | . | 1 | 1 |
|  | 1 | . | . | 1 | . | 1 | 1 | . |
| 170 | 1 | . | 1 | . | 1 | . | 1 | 1 |
|  | 1 | 1 | . | 1 | . | . | . | 1 |
|  | . | . | 1 | . | . | 1 | . | 1 |
|  | . | 1 | . | . | 1 | . | 1 | . |
|  | 1 | . | . | 1 | . | 1 | . | . |
|  | 1 | . | 1 | . | 1 | 1 | 1 | 1 |
|  | 1 | 1 | . | 1 | 1 | . | . | 1 |
|  | . | . | 1 | 1 | . | 1 | . | 1 |
|  | . | 1 | 1 | . | 1 | . | 1 | . |
|  | 1 | 1 | . | 1 | . | 1 | . | . |
| 180 | . | . | 1 | . | 1 | 1 | 1 | 1 |
|  | . | 1 | . | 1 | 1 | 1 | 1 | . |
|  | 1 | . | 1 | 1 | 1 | 1 | . | . |
|  | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
|  | . | 1 | 1 | 1 | 1 | . | . | 1 |
|  | 1 | 1 | 1 | 1 | . | . | 1 | . |
|  | . | 1 | 1 | . | . | . | 1 | 1 |
|  | 1 | 1 | . | . | . | 1 | 1 | . |

Figure 22a. The continuation of the $B_A$ matrix of Fig. 17.

|  | 7 6 5 4 3 2 1 0 |  | 7 6 5 4 3 2 1 0 |  |
|---|---|---|---|---|
| 13 | . . 1 1 1 1 . 1 |  |  |  |
| 26 | . 1 . . . . 1 1 | 2·13 | . 1 . . . . 1 1 |  |
| 39 | . . 1 1 . . . 1 | 3·13 | . . 1 1 . . . 1 |  |
| 52 | 1 1 . 1 1 . . . |  |  | $A^{13}$ satisfies (8,6,3,2,0) |
| 65 | . . 1 . 1 . 1 1 |  |  |  |
| 78 | . . . 1 . . 1 1 | 6·13 | . . . 1 . . 1 1 |  |
| 91 | 1 . . 1 1 . . 1 |  |  |  |
| 104 | . 1 1 . . . . . | 8·13 | . 1 1 . . . . . |  |
|  |  |  |  |  |
| 19 | . 1 1 1 . 1 1 . |  |  |  |
| 38 | 1 1 . 1 1 . 1 1 |  |  |  |
| 57 | . 1 1 1 1 1 1 . | 3·19 | . 1 1 1 1 1 1 . |  |
| 76 | . 1 1 . . 1 . 1 |  |  | $A^{19}$ satisfies (8,7,5,3,0) |
| 95 | 1 . 1 1 1 . 1 . | 5·19 | 1 . 1 1 1 . 1 . |  |
| 114 | 1 . . 1 1 . 1 1 |  |  |  |
| 133 | 1 . . 1 1 1 . . | 7·19 | 1 . . 1 1 1 . . |  |
| 152 | . 1 . 1 1 . . 1 | 8·19 | . 1 . 1 1 . . 1 |  |
|  |  |  |  |  |
| 23 | 1 1 1 1 1 . 1 1 |  |  |  |
| 46 | 1 1 1 1 . . . . | 2·23 | 1 1 1 1 . . . . |  |
| 69 | . . 1 1 1 . . 1 | 3·23 | . . 1 1 1 . . 1 |  |
| 92 | 1 . 1 1 . 1 . 1 |  |  | $A^{23}$ satisfies (8,5,3,2,0) |
| 115 | 1 . 1 1 . . . 1 | 5·23 | 1 . 1 1 . . . 1 |  |
| 138 | . 1 . 1 . . 1 1 |  |  |  |
| 161 | 1 . . 1 1 1 . 1 |  |  |  |
| 184 | . 1 1 1 1 . . 1 | 8·23 | . 1 1 1 1 . . 1 |  |
|  |  |  |  |  |
| 37 | 1 . 1 . 1 1 1 . | 1·37 | 1 . 1 . 1 1 1 . |  |
| 74 | 1 . 1 1 1 . 1 1 | 2·37 | 1 . 1 1 1 . 1 1 |  |
| 111 | 1 1 1 . . . . . |  |  | $A^{37}$ satisfies (8,7,6,5,2,1,0) |
| 148 | . . 1 . 1 1 . 1 |  |  |  |
| 185 | 1 1 1 1 . . 1 . | 5·37 | 1 1 1 1 . . 1 . |  |
| 222 | . . 1 1 . . 1 . | 6·37 | . . 1 1 . . 1 . |  |
| 4 | . . . 1 . . . . | 7·37 | . . . 1 . . . . |  |
| 41 | 1 1 . . . 1 . . | 8·37 | 1 1 . . . 1 . . |  |
|  |  |  |  |  |
| 43 | . . . 1 1 1 1 . |  |  |  |
| 86 | 1 1 . 1 . . 1 1 |  |  |  |
| 129 | . 1 1 . 1 . . . |  |  |  |
| 172 | . . 1 . . 1 . 1 | 4·43 | . . 1 . . 1 . 1 | $A^{43}$ satisfies (8,6,5,4,0) |
| 215 | 1 . 1 . 1 . . . | 5·43 | 1 . 1 . 1 . . . |  |
| 3 | . . . . 1 . . . | 6·43 | . . . . 1 . . . |  |
| 46 | 1 1 1 1 . . . . |  |  |  |
| 89 | 1 . . . . 1 . . | 8·43 | 1 . . . . 1 . . |  |

Figure 22b. Continuation of the identification of the polynomials

Figure 22: Continuation of Fig. 17, the Method of Identifying the Polynomials with the Similarity Classes of Equation (38)

# REFERENCES

1. R. Price and P. E. Green, Jr., "A Communication Technique for Multipath Channels," Proc. I.R.E., March 1958, p. 555.

2. W. M. Siebert, "A Radar Detection Philosophy," I.R.E. Transactions on Information Theory, 1956 Symposium Record, Vol. IT-2, #3, September, 1956.

3. Arithmetic Operations in Digital Computers, R. K. Richards, D. Van Nostrand Co., 1955, p. 144-148.

4. Neal Zierler, Several Binary-Sequence Generators, Tech. Report No. 95, Lincoln Labs., M.I.T., September 12, 1955.

5. Stoll, R. R., Linear Algebra and Matrix Theory, McGraw-Hill Book Co., 1952, p. 200.

6. Thrall, R. M. and Tornheim, L., Vector Spaces and Matrices, John Wiley and Sons, Inc., 1957.

# LIST OF SYMBOLS

$A$ = n x n matrix applying to a given shift-register connection, either simple or multiple-return.

$A_s$= n x n matrix for simple shift-register.

$B_A$= n x $\ell$ matrix related to the A matrix and expresses all the powers of A in terms of the first n-1 powers.

$C$ = any n x n matrix which relates the sequences in a set of non-maximal sequences.

$c_i$= general coefficients of algebraic polynomial from the field mod-2.

$C(\xi)$ = characteristic polynomial.

$\ell$ = length or period of impulse response sequence.

$L$ = length or period of any maximal sequence.

$n$ = number of stages in any shift-register generator.

$p$ = length or period of any general digital sequence.

$P$ = maximal length or period corresponding to a given n number of stages.

$p_n(\xi)$ = general polynomial of $n^{th}$ degree.

$u,v,w,x,y,z$ = reference to any entire sequence.

$U,V,W,X,Y\cdots Z$ = reference to any n digits of the $u,v,x\cdots z$ sequences.

$u_i(j)$ = contents of the $i^{th}$ cell of the u sequence after j shifts.

$U(k)$ = register content vector of the u sequence after k shifts.

$\xi$ = general indeterminant.

$\phi(k)$ = Euler's phi-function.

$\rho(k)$ = auto-correlation function.

[ ] = symbol for feedback connections

( ) = symbol for characteristic polynomial