C H A P T E R I

SEQUENTIAL BEHAVIOUR OF AUTONOMOUS LINEAR BINARY FEEDBACK SHIFT REGISTER

		Page
1.1	Introduction	2
1.2	Functioning of the autonomous binary feedback shift register	4
1.3	Modulo-2 addition and its properties	9
1.4	Maximal and nonmaximal shift register sequences	14
1.5	Characteristic delay polynomials and their null sequences	16
1.6	Methods of evaluating null sequences of a delay polynomial	35
1.7	Determination of delay polynomial from its null sequence	82
1.8	Properties of delay polynomials and their null sequences	101
1.9	Generation of maximal and nonmaximal linear binary sequences and study of their statistical characteristic	129
1.10	Principal areas of application and advantages of binary shift register sequences	143
1.11	Summary	149

SEQUENTIAL BEHAVIOUR OF AUTONOMOUS LINEAR BINARY FEEDBACK SHIFT REGISTER

1.1 INTRODUCTION

Considerable interest has developed during the past two decades in the binary feedback shift registers. These devices are capable of generating cyclic sequences possessing statistical properties which closely approximate those of binary random noise. (Golomb 1955, Huffman 1956, Green 1958, Young 1958, Zierler 1959, Campbell 1959, Bell 1960, Scholefield 1960, Heath 1961, Tyryn 1961, Corran and Cummins 1962, Roberts 1963, Shiva Shanker 1963, Bernfield 1964, Chow 1964, Tsao 1964, Briggs et al. 1964-65, Kramer 1965, Davies WDT 1966, Everett 1966, Godfrey 1966, 67, 68, 69, 70, Anna Tomescu 1970, and so forth). Such, apparently random, but deterministic sequences may be used, therefore, in place of this noise; and the results which are thus obtained are much more accurate than those obtained using binary noise. The ease and simplicity in generating and processing the sequences are further responsible for this development. Initially, much of this interest pertained to the use of the sequences in

the following areas :

(i) Simmulation of noise in a repeatable manner (Kramer 1965).

(ii) Synchronization of telemetry codes (Barker 1953, Gilbert 1960).

(iii) Improvement of power content of radar signals without deterioration of their power (Siebert 1956, Skewart 1959).

(iv) Communication systems (Price and Green 1958).

(v) Automatic error - correction circuits (Huffman 1956, Green and San Soucie 1958).

(vi) Counting and frequency division (Eldert 1958, Heath 1960).

(vii) Random number generation (Johnson 1959).

More recently, and to an appreciable extent, this interest has shifted to control system applications, particularly in the area of system identification. (References related to this field are given in the chapters 2, 3, 4, 5 and 6, where the subject is dealt with). These binary sequential networks are also of theoretical significance to the study of more general sequential networks.

This chapter is concerned with the theoretical analysis and experimental verification of the sequential behaviour

of autonomous linear binary feedback shift register. At first, the functioning of a feedback shift register (fsr) is presented. A brief account of the linear feedback function 'modulo-2 addition'is then given. The meaning and classification of the characteristic polynomial of the above shift-register sequence (also known as null - sequence, Huffman 1956) and of the shift - register which produced it, are stated. Methods are then described to evaluate all the possible null sequences associated with a given characteristic polynomial irrespective of its factorable features. The problem of determining the characteristic polynomial corresponding to a given null sequence is also studied. Useful properties of the characteristic polynomials and their associated null sequences are discussed, some in detail. The maximum length linear binary null sequences (also known by such names as pseudorandom binary sequences, m-sequences or simply chain codes) and the nonmaximum length binary sequences are generated, and many of their properties verified. In addition, mention is made of the principal areas of application and advantages of the binary feedback shift register sequences.

1.2 FUNCTIONING OF AN AUTONOMOUS BINARY FEEDBACK SHIFT REGISTER

A general block diagram of an autonomous binary feedback

shift register is shown in Fig. 1.1. As seen, there is no input present except a clock pulse of period t_o. Each of the rectangles labelled D_1, D_2 ... D_n is a binary storage element (flip-flop, position on a delay line, or other memory device), which delays the variable on which it operates by a period t_o. If t_o is chosen as the standard to express the amount of delay, each storage or delay element causes the delay of one unit or one clotk-pulse period. Thus, a delay of n units, D^n, may be obtained by connecting n identical delay-elements in series as shown in the figure. The number of stable states of each storage element is assumed to be ' 2 ', which remains to be the same for all devices comprising the autonomous network. At periodic intervals determined by the master-clock, the contents of D_i is transferred into D_{i+1}. The time of operation is the same regardless of the number of elements in the system. In the absence of the feedback logical path, the series string of binary delay elements gets emptied by the end of nth clock-pulse. However, the system can be kept active by feeding back outputs of some or all of the n-delay elements into the first delay element through a feedback logic device. That is, leads from some or all of the n-delay elements feed into a logic device, which provides input to the first delay element.

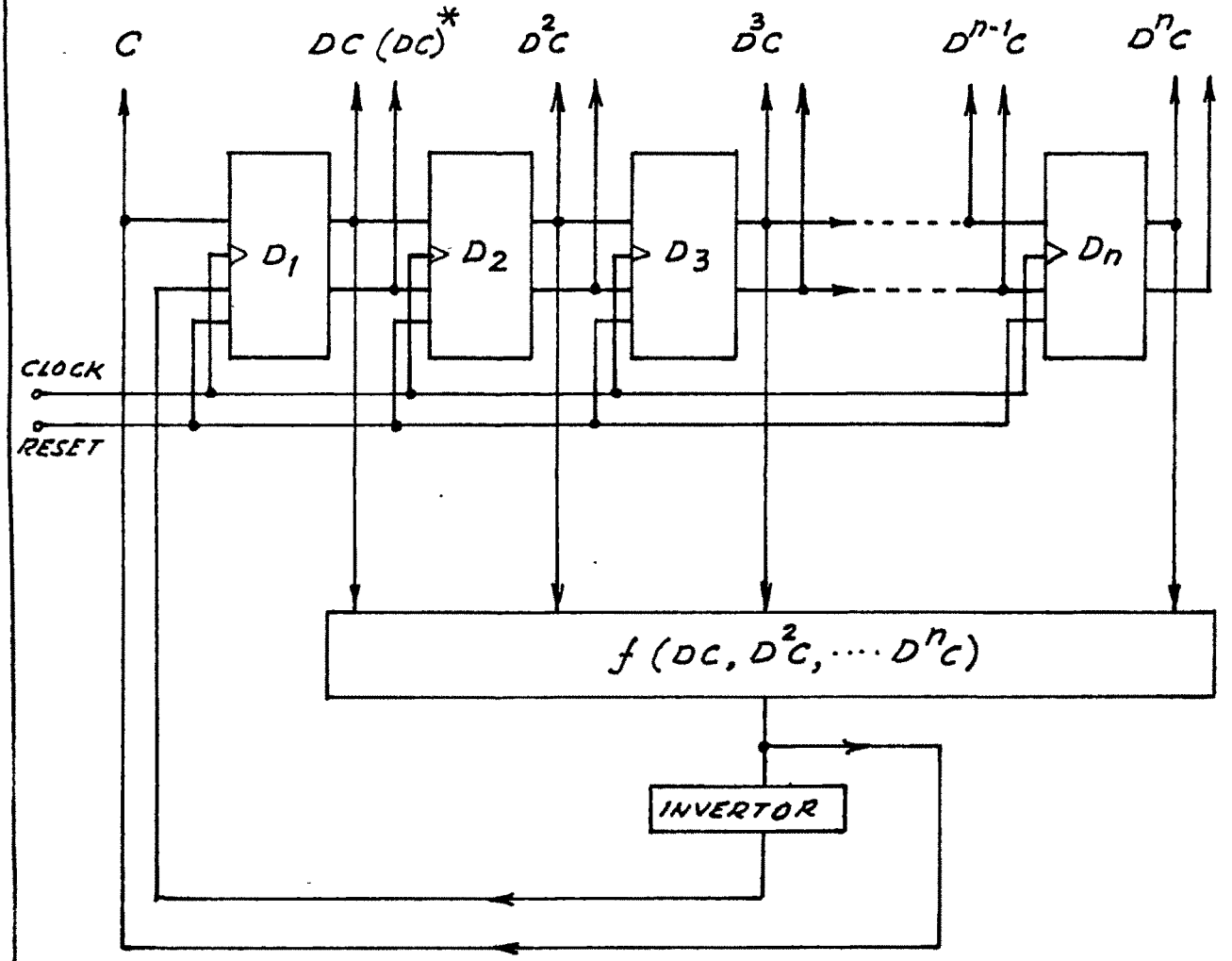


FIG. 1·1 GENERAL SHIFT REGISTER OF DEGREE n WITH LOGICAL FEEDBACK

These storage or delay elements are called the 'stages' of the system. If n stages are employed, the system or the feedback shift register (abbreviated as 'fsr') is said to be of degree n. The content at any instant of time of the n-stages is called the 'state' of the fsr, which may be thought of as a binary number. Clearly, the maximum number of distinct possible states of the n-stage fsr is 2^n (the binary numbers 00 .... 0 to 11 .... 1). On application of a train of clock - pulses, the feedback shift register undergoes, from its initial state, a cyclic succession of states, the number of which is dependent upon the nature of 'feedback function' and the initial state of the fsr. Thus, a binary sequence of certain period may be realized at the output of each stage of the shift register.

In brief, an autonomous binary feedback shift register of degree n is a device consisting of n consecutive binary storage positions, which shifts the contents of each position to the next position down the line, in time to the regular beat of a clock (or other timing device), this process being kept active by feeding back the states of certain or all of the n storage elements into the first storage element

by means of a two-state logic device. Hence, the feedback shift register may be understood as a sequential network or sequence generator which provides a cyclic sequence containing some well-defined basic number of binary digits. The following example illustrates the above idea :

Example 1.1

Consider the four-stage shift register with the feedback function expresed as

$$f(DC,\ D^2C,\ D^3C,\ D^4C) = (DC.D^2C)(D^4C)^* + (DC.D^2C)^*\ (D^4C)$$

whereby ' + ' represents the logical OR function, and the symbol * stands for the binary complementation.

The 4th degree fsr with the specified feedback function is depicted in Fig. 1.2. Table 1.1 shows the various possible cyclic outputs realizable from the given fsr with different initial states.

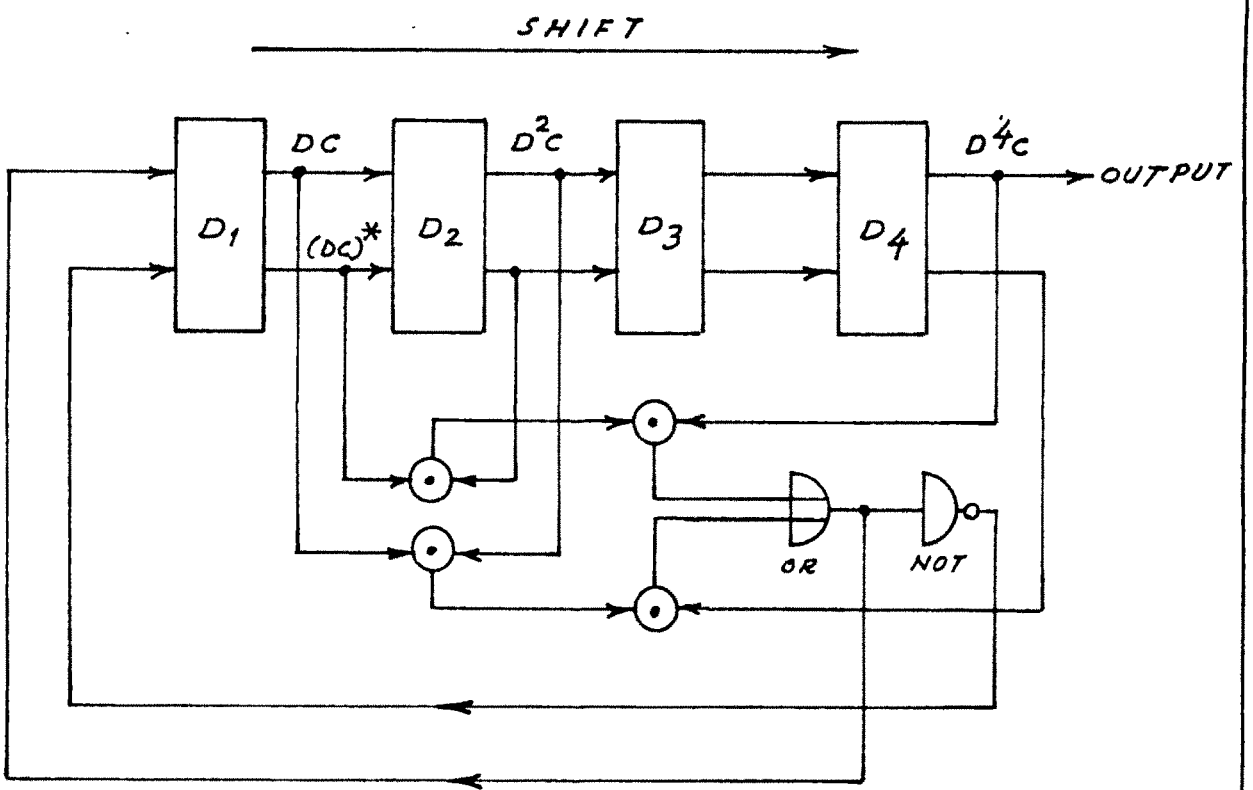


FIG. 1·2 CIRCUIT IMPLEMENTATION OF FEEDBACK FUNCTION OF EXAMPLE 1·1

Table 1.1

	Description of state of the fsr	Stage number of fsr			
		1	2	3	4
(i)	Initial state (first initial setting of the fsr)	1	1	1	1
	Second state	0	1	1	1
	Third state	1	0	1	1
	Fourth state	1	1	0	1
	Fifth state	0	1	1	0
	Sixth state	0	0	1	1
	Seventh state	1	0	0	1
	Eighth state	1	1	0	0
	Ninth state	1	1	1	0
	Tenth state	1	1	1	1
					Repeats
(ii)	Initial state (second initial setting of the fsr)	0	0	0	1
	Second state	1	0	0	0
	Third state	0	1	0	0
	Fourth state	0	0	1	0
	Fifth state	0	0	0	1
					Repeats
(iii)	Initial state (third initial setting of fsr)	0	1	0	1
	Second state	1	0	1	0
	Third state	0	1	0	1
					Repeats

The content of Table 1.1 reveals that essentially three cyclic sequences (excluding the all zero sequence), namely, 101100111, 0100, and 01, are realizable from the given fsr with the initial states '1111', '0001', and '0101'respectively.

Hence, the feedback function and the initial state determine the cyclic output from a feedback shift register. In the following section the meaning of the 'linear feedback function' known commonly by the name 'modulo-2 addition', and a few of its important properties are enumerated.

1.3 MODULO-TWO ADDITION AND ITS PROPERTIES

If $C = (c_0 , c_1 , c_2 \ldots .)$ represents the binary periodic output sequence of the feedback logic device shown in Fig. 1.1 (i.e. the input sequence to the first stage of the system), the feedback shift register may be described by the following equation :

$$f(DC, D^2C, \ldots , D^nC) = C \quad .. \quad .. \quad ..(1.1)$$

The eqn. (1.1) is thus seen to characterize the sequential behaviour of the fsr and is accordingly called as its 'Characteristic-Equation'.

However, if the feedback logic may be expressed in the form :

$$f(DC, D^2C, \ldots D^nC) = (a_1 DC \oplus a_2 D^2C \oplus \ldots \oplus a_n D^nC) \quad \ldots (1.2)$$

where each of the constants a_i is either 0 or 1, and where the symbol $\oplus$ denotes addition modulo-2 (that is, 1 for odd sums and 0 for even sums), the autonomous network of Fig. 1.1 is called 'linear'. Accordingly, the fsr under consideration is called 'linear feedback shift register'. Such a linear shift register is depicted in Fig. 1.3. Linear shift registers are linear in this standardized sense. However, the underlying arithmetic is not that of the real or complex numbers, but of the field of two elements 0 and 1, operating modulo-2. It should be noted here, that a value of '1' for any feedback coefficient $a_i (1 \leq i \leq n)$, means that the corresponding output is connected to the modulo-2 logical adder, and likewise, a value of '0' for any coefficient means that the corresponding stage output is not feedback.

The binary logical operation 'modulo-2 addition' has, some of the properties of both 'addition' and 'substraction' as shown in Table 1.2 below :

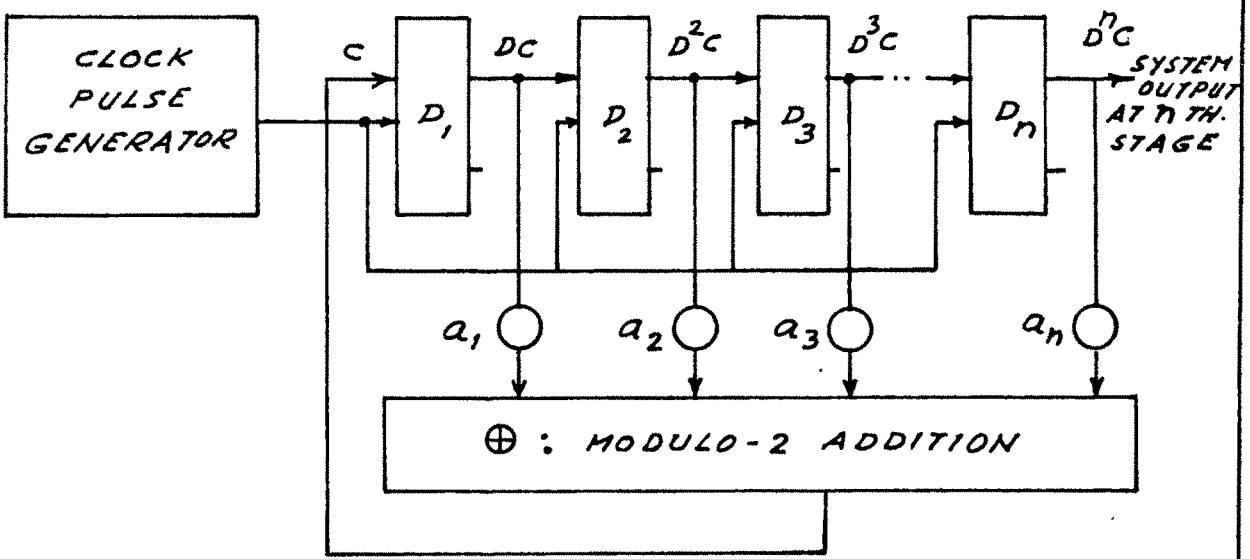


FIG. 1·3 GENERAL DIAGRAM OF AN AUTONOMOUS LINEAR BINARY FEEDBACK SHIFT REGISTER

Table 1.2

Logical Multiplication			Logical Addition			Modulo-2 Addition		
.	0	1	+	0	1	⊕	0	1
0	0	0	0	0	1	0	0	1
1	0	1	1	1	1	1	1	0

Evidently, the modulo-2 addition is the same as the 'Not - equivalent ' logical operation. The practical realization of the binary not-equivalent circuit is discussed in section (1.9.2).

Some properties of 'modulo-2 addition

The following theorems are important in connection with the operation of modulo-2 addition. Here, C_1, C_2, C_3 . . are to be treated as variables having a value of either a '1' or a '0'.

1. $C \oplus C \oplus \ldots \oplus C = 0$, Even number is added.
2. $C \oplus C \oplus \ldots \oplus C = C$, odd number is added.
3. $C_1 \oplus C_2 \oplus C_3 \oplus \ldots\ldots = 0$, if an even number of the variables C_1, C_2, C_3 .. have the value 1.
4. $C_1 \oplus C_2 \oplus C_3 \oplus \ldots\ldots = 1$, if an add number of hhe variables C_1, C_2, C_3 have the value 1.
5. $C_1 \oplus C_2 = C_2 \oplus C_1$, Commutative property of $\oplus$
6. $(C_1 \oplus C_2) \oplus C_3 = C_1 \oplus (C_2 \oplus C_3) = C_1 \oplus C_2 \oplus C_3$

   Associative property of $\oplus$.
7. $C_1C_2 \oplus C_1C_3 = C_1(C_2 \oplus C_3)$, Distributive property of $\oplus$ with Multiplication.
8. $C_1 \oplus C_2 = C_3$ implies :

   $C_1 \oplus C_3 = C_2$ and

   $C_2 \oplus C_3 = C_1$ and

   $C_1 \oplus C_2 \oplus C_3 = 0$

The following example is meant to illustrate the sequential behaviour of an autonomous linear binary shift register with modulo-2 feed back.

Example 1.2

Consider the three - stage shift register shown in Fig. 1.4, where the modulo-2 sum of 1st and 3rd stages provides input to the 1st stage.

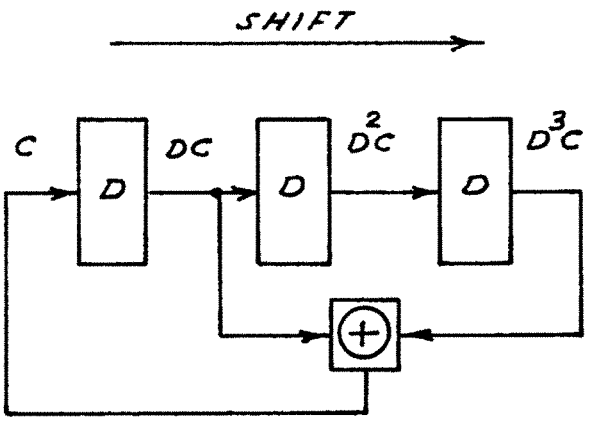


FIG. 1·4 a THREE-STAGE SHIFT REGISTER WITH MOD-2 FEEDBACK

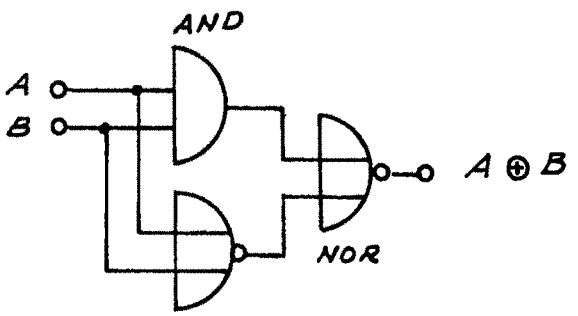


FIG. 1·4 b REALIZATION OF MOD-2 LOGICAL ADDITION WITH 1-AND AND 2-NOR

The feedback function is thus given by :

$$f(DC,\ D^2C,\ D^3C) \ = \ (DC \oplus D^3C)$$

Assuming the initial state of the linear fsr as 111, the succession of states is as follows -

Table 1.3

State of the fsr	Stage of the fsr			
	1	2	3	
Initial state	1	1	1	$1 \oplus 1 = 0$ enters 1st stage etc.
Second state	0	1	1	
Third state	1	0	1	
Fourth state	0	1	0	
Fifth state	0	0	1	
Sixth state	1	0	0	
Seventh state	1	1	0	
Eighth state	1	1	1	Repeats

The cyclic sequence obtained from any stage is .... 1010011 ... and has a period of 7 digits. In fact, the same sequence (in this special case) would have been generated by the fsr had any other initial state been assumed with the exception of all-zero initial state. The

all-zero initial state represents trivial solution as the chosen linear feedback function, namely modulo-2 addition, is ineffective to all-zero state of the fsr.

It is worth noting here, as long as the feedback operation is restricted to modulo-2 addition (i.e. multiplication is not permitted), the shift register is is a linear device and must be expected to obey the usual laws of linear devices, e.g. the law of superposition.

1.4 MAXIMAL AND NONMAXIMAL SHIFT REGISTER SEQUENCES

The sequence obtained from the autonomous linear feedback shift register is seen to depend on both the feedback connections and on the initial loading of the shift register. This leads to a grouping of the so generated sequences into two categories:

(i) Maximum - length sequences
(ii) Nonmaximum - length sequences.

The grouping depends on the length or period of the sequence. This maximum length or period of the sequence depends on the number of stages incorporated into the feedback shift register. Each storage element, being bistable, can store only two distinct ihformations. Since the shift register contains n such storage elements, there is a total of 2^n

different possible states (informations) and of all these could be generated the sequence length would be 2^n digits. However, with modulo-2 addition operation, the all-zero state must be excluded. Hence, the largest possible period for a linear binary n-stage shift register is $(2^n - 1)$ digits. If an output sequence has a period $N = (2^n - 1)$ binary digits, the sequence is called a 'maximum length binary sequence' (abbreviated as m-sequence). And, any output sequence of length less than the maximum period is accordingly called as 'nonmaximum length binary sequence.'

The maximum-length binary sequences are also known by such names as pseudorandom binary sequences, chain-codes and some less frequently used terms.

The nonmaximal binary sequences are, likewise, also called as short sequences or short chain-codes.

Now, the sequential behaviour of the linear fsr may be described by means of what is called 'characteristic delay polynomial', the meaning and classification of which now follows.

1.5 CHARACTERISTIC DELAY POLYNOMIALS AND THEIR NULL-SEQUENCES

1.5.1 The characteristic polynomial of an fsr

The describing equation for the autonomous linear shift register of Fig. 1.3 may be written as :

$$(a_1 D \oplus a_2 D^2 \oplus .... \oplus a_n D^n) C = C \quad ... \quad .... \quad (1.3)$$

whereby $C = (c_o, c_1, c_2 .....)$ represents the binary periodic output sequence of the feedback logic device (i.e. input sequence for the 1st stage of the fsr), and where each of the coefficients 'a_i' ($1 \leq i \leq n$) is either 1 or 0 depending on whether the corresponding stage is connected to the feedback logic device or otherwise.

In accordance with the modulo-2 arithmetic, stated in brief in section 1.3, the eqn.(1.3) may also be written as :

$$(I \oplus a_1 D \oplus a_2 D^2 \oplus ... \oplus a_n D^n) C = 0 \quad ... \quad ... \quad (1.4)$$

where $I \equiv D^o$ is the identity operator.

Since the system is binary, for it to be of nth degree, the coefficient 'a_n' must necessarily be unity. Hence, eqn. (1.4) becomes :

$$(I \oplus a_1 D \oplus a_2 D^2 \oplus .... \oplus a_n D^n) C = 0 \quad .. \quad .. \quad (1.5)$$

Clearly, the above eqn. (1.5) characterizes the sequential behaviour of the feedback shift register and is accordingly called as its 'characteristic-equation.'

Now, the expression within the brackets in eqn.(1.5), which is composed of characteristic delays acting on the variable C, is called 'characteristic delay polynomial of the feedback shift register, and is represented by F(D). Accordingly, the characteristic delay polynomial or simply the delay polynomial F(D) may be written as :

$$F(D) = (I \oplus a_1 D \oplus a_2 D^2 \oplus \ldots \oplus a_n D^n) \quad \ldots (1.6)$$

In closed - form, F(D) appears as :

$$F(D) = \oplus \sum_{i=0}^{n} a_i D^i \quad , \quad \text{with} \quad a_o = a_n = 1,$$

where the symbol ' $\oplus$ ' before summation indicates that it is 'addition modulo-2'.

1.5.2 Null-sqauence of a delay polynomial

Referring back to the autonomous libear shift register of Fig. 1.3, it is seen that even though no input is present, the presence of feedback paths permits a steady state output (with any nontrivial initial state).

This unforced steady state response, C, of the fsr is that for which [F (D)] C equals zero. This natural response C is hence called a null sequence of the linear shift register or of the delay polynomial F(D) that characterizes its (the fsr's) sequential behaviour.

In brief, the output sequence of an autonomous feedback shift register represents its null sequence. If this output sequence is of maximum length (section 1.4), it is called 'maximum length null sequence (mlns)' or maximum length sequence or simply m-sequence. 'Pseudorandom binary sequence', and 'chain-code' are the other names, frequently referred to, of this mlns.

The null sequence of a delay polynomial is thus periodic with a period N which depends on the shift register logical configuration and its initial state. A delay polynomial may have several distinct null sequences. These null sequences are also called the solutions of the polynomial F(D).

1.5.3 Classification of delay-polynomials

Broadly speaking, the characteristic delay polynomials, that describe the sequential behaviour of the feedback shift register, may be classified based on their factorable features.

(in the modulo-2 sense) into three groups as under :

(A) Primitive and irreducible delay polynomials

(B) Irreducible but nonpromitive delay polynomials

(C) Factorable delay polynomials.

(A) Irreducible and primitive delay polynomials

A delay polynomial is said to be irreducible and primitive, modulo-2, if and only if,

(i) The polynomial is irreducible, i.e. it has no factors (modulo - 2); and

(ii) The polynomial of degree n is not a factor of $D^K \oplus 1$ for any $K \leq 2^n - 1$.

Clearly, the solution of an irreducible and primitive delay polynomial of degree n is of period $2^n - 1$ digits and is therefore a maximum length null sequence.

To illustrate this idea of 'irreducibility and primitiveness' of a characteristic delay polynomial, the following example is given.

Example 1.3

Consider an irreducible and primitive binary delay polynomial of degree 4 given by :

$$F(D) = I \oplus D \oplus D^4$$

The irreducibility of this polynomial can be demonstrated by attempting to divide into it each possible polynomial of degree 3 or less. Further, it can also be verified that the given polynomial is not a factor of $D^K \oplus I$ for any $K < 2^4 - 1$.

Hence, the given polynomial is an irreducible and primitive modulo-2 of degree 4.

Now, the characteristic equation of the corresponding feedback shift register is :

$$[F(D)]\ C = 0$$

$$\text{i.e.}\quad (I \oplus D \oplus D^4)C = 0$$

where C is the null-sequence associated with the given polynomial, representing here the input-sequence to the 1st stage of the autonomous linear fsr.

The logical configuration of the 4-stage fsr is depicted in Fig. 1.5.

Assuming any non-zero initial state, the succession of states in the fsr is given below.

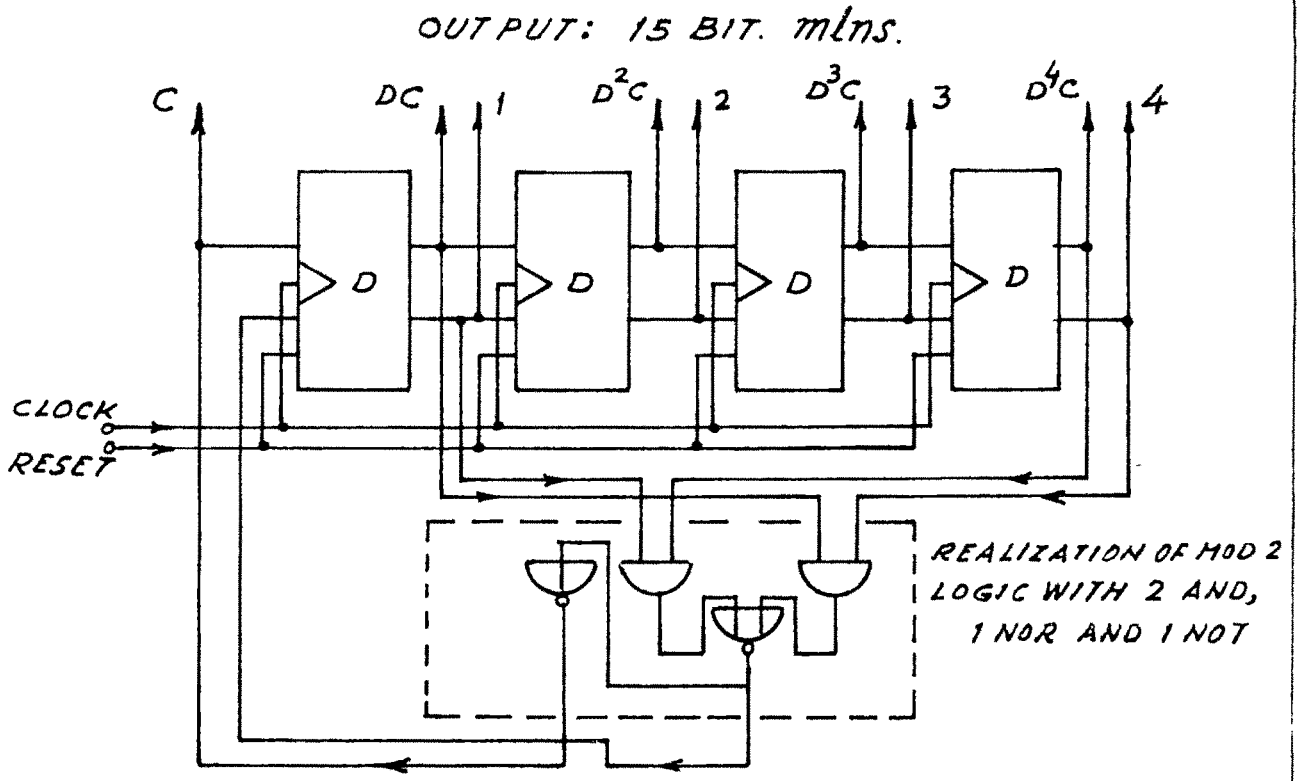


FIG. 1·5 LINEAR BINARY MAXIMUM LENGTH F.S.R. OF DEGREE 4

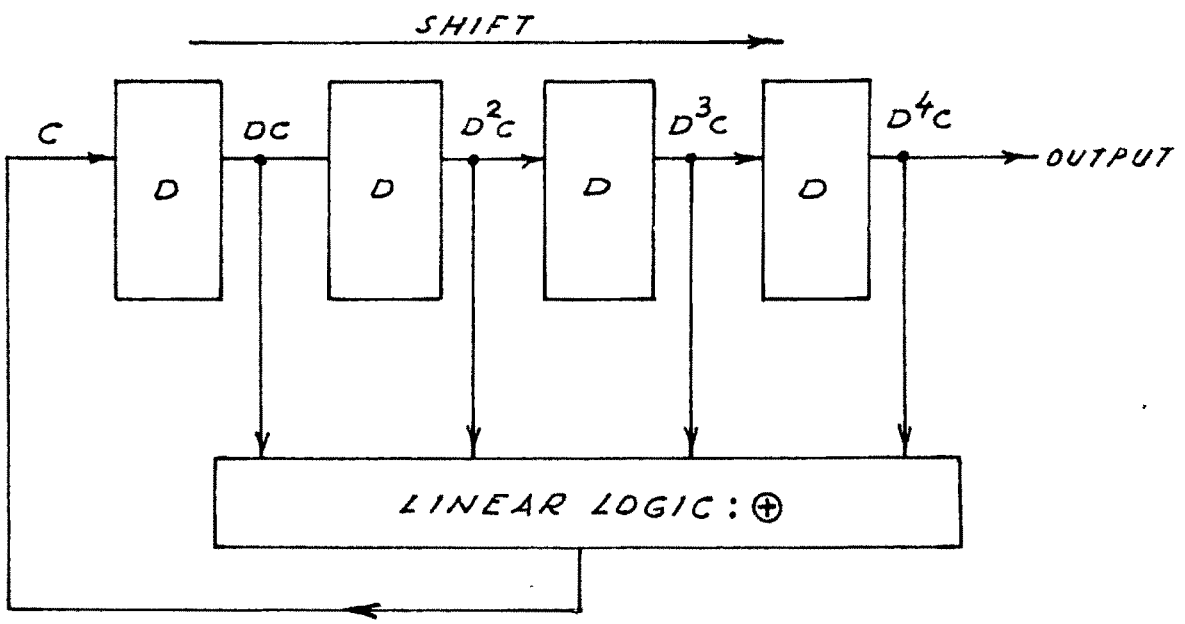


FIG. 1·6 LINEAR BINARY NONMAXIMAL F.S.R. OF DEGREE 4.

Table 1.4

State number of the fsr	Stage number of the fsr			
	1	2	3	4
First (initial) state	1	1	1	1
Second state	0	1	1	1
Third state	1	0	1	1
Fourth state	0	1	0	1
Fifth state	1	0	1	0
Sixth state	1	1	0	1
Seventh state	0	1	1	0
Eighth state	0	0	1	1
Ninth state	1	0	0	1
Tenth state	0	1	0	0
Eleventh state	0	0	1	0
Twelfth state	0	0	0	1
Thirteenth state	1	0	0	0
Fourteenth state	1	1	0	0
Fifteenth state	1	1	1	0
Sixteenth state	1	1	1	1 (Repeats)

The cyclic succession obtained from any stage is

..... , 101011001000111, ...

and has a period of $2^4 - 1 = 15$ bits. The same sequence would have been generated had any other initial state been assumed with the exception of '0000'.

Clearly, all possible different 4-digit states are encountered in the above null sequence of period $2^4 - 1$

(here n = 4) bits. Hence, the solution of an irreducible and primitive binary delay polynomial of degree n is always a maximum length null sequence of repetition period $2^n - 1$ bits.

The irreducible and primitive binary delay polynomials upto degree n = 8, some of which are treated in the later sections of this chapter, are given in tabular form below. An exhaustive list of irreducible polynomials, upto degree 30, indicating those which are primitive, may be found in Peterson (1961).

Table 1.5 :

Degree of F(D), n	Irreducible and primitive Polynomial F(D)	Period of the null sequence in bits
2	$I \oplus D \oplus D^2$	3
3	$I \oplus D \oplus D^3$	7
3	$I \oplus D^2 \oplus D^3$	7
4	$I \oplus D \oplus D^4$	15
4	$I \oplus D^3 \oplus D^4$	15
5	$I \oplus D \oplus D^2 \oplus D^3 \oplus D^5$	31
5	$I \oplus D \oplus D^3 \oplus D^4 \oplus D^5$	31
5	$I \oplus D \oplus D^3 \oplus D^4 \oplus D^5$	31
5	$I \oplus D^2 \oplus D^5$	31

(Table 1.5 continued)

Degree of F(D), n	Irreducible and primitive polynomial, F(D)	Period of the null sequence in bits
5	$I \oplus D^2 \oplus D^3 \oplus D^4 \oplus D^5$	31
5	$I \oplus D^3 \oplus D^5$	31
6	$I \oplus D \oplus D^6$	63
6	$I \oplus D \oplus D^2 \oplus D^5 \oplus D^6$	63
6	$I \oplus D \oplus D^3 \oplus D^4 \oplus D^6$	63
6	$I \oplus D \oplus D^4 \oplus D^5 \oplus D^6$	63
6	$I \oplus D^2 \oplus D^3 \oplus D^5 \oplus D^6$	63
6	$I \oplus D^5 \oplus D^6$	63
7	$I \oplus D \oplus D^7$	127
7	$I \oplus D \oplus D^2 \oplus D^3 \oplus D^7$	127
7	$I \oplus D \oplus D^2 \oplus D^3 \oplus D^4 \oplus D^5 \oplus D^7$	127
7	$I \oplus D \oplus D^2 \oplus D^3 \oplus D^5 \oplus D^6 \oplus D^7$	127
7	$I \oplus D \oplus D^2 \oplus D^4 \oplus D^5 \oplus D^6 \oplus D^7$	127
7	$I \oplus D \oplus D^2 \oplus D^5 \oplus D^7$	127
7	$I \oplus D \oplus D^3 \oplus D^5 \oplus D^7$	127
7	$I \oplus D \oplus D^3 \oplus D^6 \oplus D^7$	127
7	$I \oplus D \oplus D^4 \oplus D^6 \oplus D^7$	127
7	$I \oplus D^2 \oplus D^3 \oplus D^4 \oplus D^7$	127

(Table 1.5 continued)

Degree of F(D), n	Irreducible and primitive polynomial, F(D)	Period of the null sequence in bits
7	$I \oplus D^2 \oplus D^3 \oplus D^4 \oplus D^5 \oplus D^6 \oplus D^7$	127
7	$I \oplus D^2 \oplus D^4 \oplus D^6 \oplus D^7$	127
7	$I \oplus D^2 \oplus D^5 \oplus D^6 \oplus D^7$	127
7	$I \oplus D^3 \oplus D^7$	127
7	$I \oplus D^3 \oplus D^4 \oplus D^5 \oplus D^7$	127
7	$I \oplus D^4 \oplus D^7$	127
7	$I \oplus D^4 \oplus D^5 \oplus D^6 \oplus D^7$	127
7	$I \oplus D^6 \oplus D^7$	127
8	$I \oplus D \oplus D^2 \oplus D^3 \oplus D^4 \oplus D^6 \oplus D^8$	255
8	$I \oplus D \oplus D^2 \oplus D^3 \oplus D^6 \oplus D^7 \oplus D^8$	255
8	$I \oplus D \oplus D^2 \oplus D^5 \oplus D^6 \oplus D^7 \oplus D^8$	255
8	$I \oplus D \oplus D^2 \oplus D^7 \oplus D^8$	255
8	$I \oplus D \oplus D^3 \oplus D^5 \oplus D^8$	255
8	$I \oplus D \oplus D^5 \oplus D^6 \oplus D^8$	255
8	$I \oplus D \oplus D^6 \oplus D^7 \oplus D^8$	255
8	$I \oplus D^2 \oplus D^3 \oplus D^4 \oplus D^8$	255
8	$I \oplus D^2 \oplus D^3 \oplus D^5 \oplus D^8$	255
8	$I \oplus D^2 \oplus D^3 \oplus D^6 \oplus D^8$	255
8	$I \oplus D^2 \oplus D^3 \oplus D^7 \oplus D^8$	255
8	$I \oplus D^2 \oplus D^4 \oplus D^5 \oplus D^6 \oplus D^7 \oplus D^8$	255

(Table 1.5 continued)

Degree of F(D), n	Irreducible and primitive polynomial, F(D)	Period of the null sequence in bits
8	$I \oplus D^2 \oplus D^5 \oplus D^6 \oplus D^8$	255
8	$I \oplus D^3 \oplus D^5 \oplus D^6 \oplus D^8$	255
8	$I \oplus D^3 \oplus D^5 \oplus D^7 \oplus D^8$	255
8	$I \oplus D^4 \oplus D^5 \oplus D^6 \oplus D^8$	255

(B) Irreducible but nonprimitive delay polynomials

An irreducible but nonprimitive, modulo-2, delay polynomial means that -

(i) The polynomial has no factors (modulo-2), but
(ii) the polynomial (of degree n) is a factor of $D^K \oplus I$ for some value of $K < 2^n - 1$.

Irreducible but nonprimitive delay polynomials occur, in general, whenever the maximal period for a given n ($= 2^n - 1$) is nonprimitive (Table 1.6). These are also called as 'nonmaximal irreducible polynomials'.

Evidently, the solution of an irreducible but nonprimitive polynomial of degree n is of period less than the maximum of $2^n - 1$ digits. This situation readily implies that a non-maximal irreducible polynomial exhibits several solutions.

However, it may be noted that all these different solutions are of the same period. In otherwords, irreducibility is sufficient to insure that all the nontrivial solutions (null sequences) be of equal length. The following examples clear these concepts.

Example 1.4

Consider an irreducible but nonprimitive binary delay polynomial of degree 4 given by :

$$F(D) = (I \oplus D \oplus D^2 \oplus D^3 \oplus D^4)$$

The irreducibility of the above polynomial can be demonstrated by attempting to divide into it each possible polynomial of degree 3 or less. Further, it can also be verified that this polynomial is a factor of $D^5 \oplus I$.

Thus, the given polynomial is certainly irreducible but nonprimitive, modulo-2.

The characteristic equation of the corresponding fsr is :

$$(I \oplus D \oplus D^2 \oplus D^3 \oplus D^4) C = 0$$

where C (as before) is the null sequence of the polynomial F(D), and represents the input sequence to the first stage of the autonomous fsr as shown in Fig. 1.6.

Assuming different initial states, the solutions of the above polynomial are tabulated below :

Table 1.6

State - Number	Stage Number				
	1	2	3	4	
First (first initial setting of the fsr)	1	1	1	1	
Second state	0	1	1	1	
Third state	1	0	1	1	
Fourth state	1	1	0	1	
Fifth state	1	1	1	0	
Sixth state	1	1	1	1	Repeats
First (second initial setting of the fsr)	1	1	0	0	
Second state	0	1	1	0	
Third state	0	0	1	1	
Fourth state	0	0	0	1	
Fifth state	1	0	0	0	
Sixth state	1	1	0	0	Repeats
First (third initial setting of the fsr)	1	0	1	0	
Second state	0	1	0	1	
Third state	0	0	1	0	
Fourth state	1	0	0	1	
Fifth state	0	1	0	0	
Sixth state	1	0	1	0	Repeats

Now, the sum of the periods of the above three distinct sequences equals 15 (= $2^4 - 1$). As these three sequences namely, 11110, 00110 and 01010, together describe all the possible $2^4 - 1$ nonzero states of the given 4th degree fsr, they represent the complete solution of the given irreducible but nonprimitive delay polynomial.

The important conclusions worthy of mention here are the following :

(i) An irreducible and nonprimitive polynomial exhibits several null sequences.

(ii) The period or the length of each null sequence is less than the maximum of $2^n - 1$ digits, n being the degree of the polynomial.

(iii) All null sequences are of equal period.

(iv) The length of all distinct null sequences equals $2^n - 1$ digits.

The table below gives the irreducible but nonprimitive delay polynomials upto degree 8, some of which are treated later in this chapter.

Table 1.7

Degree of F(D), n	Irreducible and Nonprimitive Polynomial F(D)	Period of the null sequence in bits
1	$I \oplus D$	1
4	$I \oplus D \oplus D^2 \oplus D^3 \oplus D^4$	5
6	$I \oplus D \oplus D^2 \oplus D^4 \oplus D^6$	21
6	$I \oplus D^2 \oplus D^4 \oplus D^5 \oplus D^6$	21
6	$I \oplus D^3 \oplus D^6$	9
8	$I \oplus D \oplus D^2 \oplus D^3 \oplus D^4 \oplus D^5 \oplus D^8$	85
8	$I \oplus D \oplus D^2 \oplus D^3 \oplus D^4 \oplus D^7 \oplus D^8$	51
8	$I \oplus D \oplus D^2 \oplus D^4 \oplus D^5 \oplus D^6 \oplus D^8$	85
8	$I \oplus D \oplus D^2 \oplus D^4 \oplus D^6 \oplus D^7 \oplus D^8$	17
8	$I \oplus D \oplus D^3 \oplus D^4 \oplus D^8$	51
8	$I \oplus D \oplus D^3 \oplus D^4 \oplus D^5 \oplus D^6 \oplus D^8$	85
8	$I \oplus D \oplus D^3 \oplus D^7 \oplus D^8$	85
8	$I \oplus D \oplus D^4 \oplus D^5 \oplus D^6 \oplus D^7 \oplus D^8$	51
8	$I \oplus D \oplus D^5 \oplus D^7 \oplus D^8$	85
8	$I \oplus D^2 \oplus D^3 \oplus D^4 \oplus D^5 \oplus D^7 \oplus D^8$	85
8	$I \oplus D^2 \oplus D^3 \oplus D^4 \oplus D^6 \oplus D^7 \oplus D^8$	85
8	$I \oplus D^4 \oplus D^5 \oplus D^7 \oplus D^8$	51
8	$I \oplus D^3 \oplus D^4 \oplus D^5 \oplus D^8$	17
8	$I \oplus D^3 \oplus D^4 \oplus D^5 \oplus D^6 \oplus D^7 \oplus D^8$	85

(C) Factorable delay polynomials

A factorable delay polynomial (modulo - 2) is one which is reducible into two or more irreducible polynomials (modulo-2). Accordingly, the null sequences of the factorable polynomial depend on the nature and degrees of its factors.

To illustrate the nature of null sequences of factorable polynomials, the results obtained for the polynomials in the following cases :

(i) Polynomial with nonrepeated factors only

(ii) Polynomial with repeated factors only, and

(iii) Polynomial with repeated and nonrepeated factors,

are given in tabular form below :

Table 1.8 (Polynomial with nonrepeated factors)

$$F(D) = I \oplus D^2 \oplus D^3 \oplus D^4$$

$$= (I \oplus D)(I \oplus D + D^3)$$

Characteristic equation of the corresponding fsr is :

$(I \oplus D^2 \oplus D^3 \oplus D^4)\, C = 0$, where C is the null sequence associated with F(D).

Table 1.8 (continued)

State number of the fsr	stage Number of the fsr				Remarks
	1	2	3	4	
First state (first initial setting of the fsr)	1	1	1	1	1st null sequence of F(D). With period N_1 = 1 bit.
Second state	1	1	1	1 (repeats)	
First state (second initial setting of fsr)	1	0	0	0	
Second state	0	1	0	0	
Third state	1	0	1	0	
Fourth state	1	1	0	1	2nd null sequence of F(D) with period N_2= 7bits.
Fifth state	0	1	1	0	
Sixth state	0	0	1	1	
Seventh state	0	0	0	1	
Eighth state	1	0	0	0 (repeats)	
First state (Third initial setting of fsr)	1	1	0	0	
Second state	1	1	1	0	
Third state	0	1	1	1	
Fourth state	1	0	1	1	3rd null sequence of F(D) with period N_3= 7 bits
Fifth state	0	1	0	1	
Sixth state	0	0	1	0	
Seventh state	1	0	0	1	
Eighth state	1	1	0	0 (repeats)	

period of all distinct null sequences of F(D) = $N = N_1 + N_2 + N_3$
= 1 + 7 + 7= 15

Table 1.9 : (Polynomial with only repeated factors)

$$F(D) = (I \oplus D \oplus D^2)^2$$

Characteristic eqn. of fsr : $(I \oplus D \oplus D^2)^2 C = 0$ where C is the null sequence of F(D).

State number of the fsr	stage number of fsr 1	2	3	4	Remarks
First state (1st initial setting of fsr)	1	1	1	1	
Second state	0	1	1	1	
Third state	0	0	1	1	
Fourth state	1	0	0	1	1st null sequence of F(D) with period N_1 = 6 bits
Fifth state	1	1	0	0	
Sixth state	1	1	1	0	
Seventh state	1	1	1	1 (repeats)	
First state (2nd initial setting of fsr)	1	0	0	0	
Second state	0	1	0	0	
Third state	1	0	1	0	
Fourth state	0	1	0	1	2nd null sequence of F(D) with period N_2 = 6 bits
Fifth state	0	0	1	0	
Sixth state	0	0	0	1	
Seventh state	1	0	0	0 (repeats)	
First state (3rd initial setting of fsr)	1	1	0	1	
Second state	0	1	1	0	
Third state	1	0	1	1	3rd null sequence of F(D) with period N_3 = 3 bits
Fourth state	1	1	0	1 (repeats)	

Period of all distinct sequences of F(D) = $N = N_1 + N_2 + N_3$
$= 6 + 6 + 3 = 15.$

Table 1.10 (Polynomial with repeated and nonrepeated factors)

$F(D) = (I \oplus D \oplus D^2)^2 (I \oplus D)$

Characteristic equation of the corresponding fsr:

$F(D)\ C = (I \oplus D \oplus D^2 \oplus D^3 \oplus D^4 \oplus D^5)\ C = 0$

State number	Stage number of fsr 1	2	3	4	5	Remarks
First state (Ist initial setting of the fsr)	1	1	1	1	1	Ist null sequence of F(D) of period N_1 = 1 bit
second state	1	1	1	1	1 (repeats)	
First state (2nd initial setting of the fsr)	0	0	0	0	1	2nd null sequence of F(D) of period N_2 = 6 bits
Second state	1	0	0	0	0	
Third state	1	1	0	0	0	
Fourth state	0	1	1	0	0	
Fifth state	0	0	1	1	0	
Sixth state	0	0	0	1	1	
Seventh state	0	0	0	0	1 (repeats)	
First stage (3rd initial setting of the fsr)	0	0	0	1	0	3rd null sequence of F(D) of period N_3 = 6 bits
Second state	1	0	0	0	1	
Third state	0	1	0	0	0	
Fourth state	1	0	1	0	0	
Fifth state	0	1	0	1	0	
Sixth state	0	0	1	0	1	
Seventh state	0	0	0	1	0 (repeats)	

(Table 1.10 continued)

State number	Stage number of fsr					Remarks
	1	2	3	4	5	
First state (4th initial setting of the fsr)	0	0	1	0	0	4th null sequence of F(D) of period N_4=3bits
Second state	1	0	0	1	0	
Third state	0	1	0	0	1	
Fourth state	0	0	1	0	0	
					(repeats)	
First state (5th initial setting of the fsr)	0	0	1	1	1	5th null sequence of F(D) of period N_5 = 6 bits
Second state	1	0	0	1	1	
Third state	1	1	0	0	1	
Fourth state	1	1	1	0	0	
Fifth state	1	1	1	1	0	
Sixth state	0	1	1	1	1	
Seventh state	0	0	1	1	1	
					(repeats)	
First state (6th initial setting of the fsr	0	1	1	0	1	6th null sequence of F(D) of period N_6 = 3 bits
Second state	1	0	1	1	0	
Third state	1	1	0	1	1	
Fourth state	0	1	1	0	1	
					(repeats)	
First state (7th initial setting of the fsr)	0	1	0	1	1	7th null sequence of F(D) of period N_7 = 6 bits
Second state	1	0	1	0	1	
Third state	1	1	0	1	0	
Fourth state	1	1	1	0	1	
Fifth state	0	1	1	1	0	
Sixth state	1	0	1	1	1	
Seventh state	0	1	0	1	1	
					(repeats)	

length of all distinct null sequences of F(D), $N = \sum_{i=1}^{7} N_i = 31$

Properties of delay polynomials and their null sequences are detailed in a later section. Some points worthy of mention at this juncture are as under :

(i) A factorable polynomial has several null sequences.

(ii) The periods of its different null sequences depend on the nature and the degrees of its factors.

(iii) The null sequences of its factors are also null sequences of the original polynomial.

(iv) The period of the null sequence of a factorable polynomial could even be less than the degree of the polynomial.

(v) Σ length of all of its distinct null sequences equals $2^n - 1$ bits, n being the degree of the polynomial.

1.6 METHODS OF EVALUATING NULL SEQUENCES OF A DELAY POLYNOMIAL

In the previous section, the nature of null sequences of a delay polynomial is studied. This section develops methods to obtain all possible null sequences, analytically, of a given delay polynomial irrespective of its factorable features. For this purpose two methods are developed. In the first method, the classic idea of ' Generating Function ' is utilized to determine the null sequences of the given polynomial and hence it is called'Generating Function Method'. In the second method

a transform denoted as ' C_k - transform ' is introduced by making use of which a ' linear recurrence ' is developed for evaluation of the null sequences. Truely speaking, these two methods are quite interrelated, and hence cannot be called distinct. However, the approaches differ. The delay polynomials are considered under three groups :

(A) Primitive polynomials

(B) Irreducible but nonprimitive polynomials

(C) Factorable polynomials.

1.6.1 Evaluation of null sequences of a delay polynomial by 'Generating Function Method'

Consider the binary sequence C represented by the successive terms $(c_o , c_1 , ... c_r, ...)$ as generated at the input terminal of the first stage of the linear feedback shift register as shown in Fig. 1.3. The theory states that, one may associate a 'Generating Function' G(x) with the null sequence C and write :

$$G(x) = \bigoplus_{r=0}^{\infty} c_r x^r \quad (\text{ ' } \oplus \text{ ' indicates modulo-2 addition }) \qquad .. \quad .. \quad (1.7)$$

From the logical feedback provided in the shift register of Fig. 1.3, any term c_r in the sequence C is a modulo-2 sum of the contents at the (r - 1)-st state.

Hence, the entire sequence C satisfies a relation of the form :

$$c_r = \bigoplus_{i=1}^{n} a_i c_{r-i} \quad .. \quad .. \quad (1.8)$$

where the coefficient a_1 , a_2 , ... a_{n-1} are all 1's and 0's, and do not depend on n and where $a_n = 1$ as the fsr is binary and of nth degree.)(Addition, of course, is modulo-2). Such a relationship is known as linear recurrence and any sequence C which satisfies eqn. (1.8) is called a linear recurring sequence.

The initial state of the fsr may be thought of as

$$c_{-1}, c_{-2}, c_{-3} \ .. \ ... \ , c_{-n} \quad .. \quad .. \quad (1.9)$$

Substituting for c_r in the eqn. (1.7) :

$$G(x) = \bigoplus_{r=0}^{\infty} \sum_{i=1}^{n} a_i c_{r-i} x^r$$

$$= \bigoplus_{i=1}^{n} a_i x^i \sum_{r=0}^{\infty} a_{r-i} x^{r-i} \quad .. \quad ..$$

$$= \bigoplus_{i=1}^{n} a_i x^i \left(c_{-i} x^{-i} \oplus \ldots \oplus c_{-1} x^{-1} \oplus \sum_{r=0}^{\infty} c_r x^r \right) \quad .. \quad (1.10)$$

The above equation may be expressed as,

$$G(x) = \frac{\oplus \sum_{i=1}^{n} a_i x^i (c_{-i} x^{-i} \oplus .... \oplus c_{-1} x^{-1})}{1 \oplus \sum_{i=1}^{n} a_i x^i} \quad .. (1.11)$$

This expresses G(x) entirely in terms of the initial conditions c_{-1}, c_{-2}, ... , c_{-n}, and the feedback coefficients a_1, a_2, ... , a_n. In fact, the denominator of eqn. (1.11) is independent of even the initial conditions.

G(x) may be written in closed form as :

$$G(x) = \frac{\oplus \sum_{i=0}^{n-1} b_i x^i}{1 \oplus \sum_{i=0}^{n} a_i x^i} \quad .. \quad .. \quad .. \quad (1.12)$$

where

$$b_j = \oplus \sum_{i=1}^{n-j} a_{i+j} c_{-i} , \quad 0 \; j \; n-1.$$

Because of the properties of modulo-2 gates (i.e. $1 \oplus 1 = 0$), the algebraic difference between plus and minus disappears. Therefore G(x) may be conveniently expressed as

$$G(x) = \left(\frac{\sum_{i=0}^{n-1} b_i D^i}{\sum_{i=0}^{n} a_i D^i}\right) x , \quad a_o = 1 \quad .. \quad (1.13)$$

with $I = D^o = 1$ as the identity operator and symbol D^i corresponding to a delay of i digits as already pointed out.

Identifying the denominator of eqn.(1.13) with the characteristic delay polynomial F(D) stated in eqn.(1.6), G(x) appears :

$$G(x) = \left(\frac{\sum_{i=0}^{n-1} b_i D^i}{F(D)}\right) x \qquad \ldots \quad \ldots \quad \ldots \quad (1.14)$$

Further, the given binary fsr may be activated from any of the $2^n - 1$ nonzero initial states. For simplicity, assuming the initial state as

$$c_{-1} = c_{-2} = \ldots = c_{1-n} = 0 \quad \text{and} \quad c_{-1} = 1,$$

G(x) reduces to its simple form as :

$$G(x) = \left(\frac{1}{F(D)}\right) x, \qquad (\text{since } a_n = 1) \ \ldots(1.15)$$

Thus, in case the initial state and the delay polynomial of the feedback shift register are specified, it is possible to find null sequence(s) associated with the polynomial. The period of the null sequence evidently depends on the initial state and type of the polynomial.

Group A : Primitive Delay Polynomials

As seen in the previous section, if the delay polynomial is primitive, the period of its null sequence equals $2^n - 1$ digits. Such a sequence is called maximum length null sequence or simply m - sequence, abbreviated as

' mlns '. Thus for a primitive polynomial, the null sequence yielded by the corresponding generating function, with any nonzero initial state, describes all the $2^n - 1$ distinct binary states of the linear fsr, and constitutes the complete set of null sequences of the polynomial. Persuading the method with any other nonzero initial state merely produces a delayed replica of the same sequence. These ideas are illustrated by means of the following example.

Example 1.6 : (A case of maximal polynomial)

Suppose that it is desired to find all the null sequences of the maximal or primitive polynomial given by :

$$F(D) = I \oplus D^3 \oplus D^4$$

Assuming the initial state as ' 0001 ' of the corresponding fsr, the generating function from eqn.(1.15) is :

$$G(x) = \frac{I}{(I \oplus D^3 \oplus D^4)}\ x$$

$$= x(I \oplus D^3 \oplus D^4 \oplus D^6 \oplus D^8 \oplus D^9 \oplus D^{10} \oplus D^{11} \oplus D^{15} \oplus D^{18} \oplus D^{19} \oplus \ldots\ldots \quad .. \quad (1.16)$$

Hence, the null sequence of F(D), C, is :

C : $1(D^0)$, $0(D^1)$, $0(D^2)$, $1(D^3)$, $1(D^4)$, $0(D^5)$, $1(D^6)$, $0(D^7)$, $1(D^8)$, $1(D^9)$, $1(D^{10})$, $1(D^{11})$, $0(D^{12})$, $0(D^{13})$, $0(D^{14})$, $1(D^{15})$, ...

= 100110101111000, 100110101111000, ... repeats.

Clearly, the sequence C is cyclic with period $N = 15 = 2^4 - 1$ digits. As C describes all possible nontrivial states of the 4th degree binary fsr, we have obtained complete solution for the given polynomial. Indeed, the solution itself indicates that the polynomial is a primitive, modulo-2.

The following table, showing the successive states, helps to derive some properties of the null sequence as obtained by the generating function method.

Table 1.11

Description of null sequence	State number of the fsr														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15,...
Output of 1st stage	0	1	0	0	1	1	0	1	0	1	1	1	1	0	0,...
Output of 2nd stage	0	0	1	0	0	1	1	0	1	0	1	1	1	1	0,...
Output of 3rd stage	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1,...
Output of 4th stage	1	0	0	0	1	0	0	1	1	0	1	0	1	1	1,...
Input to 1st stage	1	0	0	1	1	0	1	0	1	1	1	1	0	0	0,... repeat

Properties of delay polynomials and their null sequences are stated in a later section. Some points worthy of mention

here are as under :

With initial state ' 0001 ', the null sequence C, as described by the generating function G(x), starts with digit 1 and appears as the input sequence to the 1st stage (Table 1.11) in accordance with the assumption. Further, the initial state ' 0001 ' appears in the sequence C at the end of the cycle in its reverse order, as ' 1000 '. This property may be made use of to (1) determine the delay polynomial from a given null sequence with the help of equation (1.15) and (2) to regulate the succession of digits in the sequence at any stage of the system.

Group B : Irreducible but non-primitive Polynomials

In the case of the irreducible and nonpromitive polynomial, the situation is somewhat different. Here, due to its nonpromitive feature, with any nonzero initial state, the generating function G(x) gives a null sequence of nonmaximal length. As a result, such polynomials possess several null sequences or solutions. But, it is verified earlier (Section 1.5.3) that an irreducible polynomial exhibits sequences of equal period. This means each solution describes equal number of states of the corresponding fsr. If the first sequence, (say) C_1 , given by G(x) is of

period N_1, the total number of distinct sequences of the polynomial F(D) then equals $2^n - 1 / N_1$. This set of sequences, say C_i , thus constitutes the complete solution of the given polynomial. The set of sequences C_i may be realized in two ways as under :

(i) A new initial state that is not described by the first sequence C_1 may be considered, and the eqn. (1.14) may again be utilized to arrive at the second sequence. This method can be continued till the $2^n - 1 / N_1$ sequences are obtained. Such a procedure obviously involves a lot of computation.

(ii) A simpler method than the above is as follows :

The theorem below is introduced to facilitate the evaluation of all the null sequences of a given polynomial :

Theorem 1 :

If $C = (c_o, c_1 , \ldots)$ is a null sequence of period N digits associated with a linear delay polynomial F(D), then the sequences C_j described by :

$$C_j = C \oplus D^j C , \qquad (1 \leq j < N) \quad \ldots \quad \ldots \quad (1.16)$$

are also null sequences of the polynomial F(D).

This may be verified as under :

For a given delay polynomial F(D), a null sequence C is that for which

$$[F(D)]\ C = 0$$

Substituting C_j in place of C , we get

$$[F(D)]\ C_j = F(D)\ [C \oplus D^j C]$$

$$= [F(D)]\ C \oplus D^j\ [F(D)]\ C$$

$$= 0$$

Thus, for permissible values of j, C_j describes null sequences of F(D). However, only for certain values of j, C_j yields distinct or new solutions other than the already obtained sequence (using G(x)). Once the complete solution for F(D) is obtained, then, persuading the use of eqn. (1.16) for other values of 'j' merely gives shifted versions of the already obtained sequences. This must be true since a binary delay polynomial can exhibit several null sequences, but with the Σ length of all these distinct sequences equalling only $2^n - 1$ digits (with modulo-2 feedback). An example covering the situation is illustrated below :

Example 1.7 :(A case of irreducible but nonprimitive polynomial).

Consider the irreducible and nonprimitive delay polynomial F(D) written as :

$$F(D) = (I \oplus D \oplus D^2 \oplus D^3 \oplus D^4)$$

It is desired to find the null sequences associated with this polynomial.

With the initial state '0001 ', the generating function G(x) from equation (1.15) becomes :

$$G(x) = \left(\frac{I}{I \oplus D \oplus D^2 \oplus D^3 \oplus D^4} \right) x$$

$$= (I \oplus D \oplus D^5 \oplus D^6 \oplus D^{10} \oplus \ldots)$$

Hence, the null sequence C_1 of the given polynomial is :

C_1 : 11000, 11000, ...repeats;

The sequence C_1 is periodic with period N_1 equal to 5 digits, and hence is a nonmaximal sequence. To obtain other null sequences of F(D), we now utilize the expression (1.16).

With j = 1, we get the second distinct null sequence C_2 of F(D) as shown below :

Sequence C_1 :	11000, ...	(repeats)
1st delayed version of C_1, DC_1 :	01100, ...	(repeats)
$C_2 = (C_1 \oplus DC_1)$:	10101, ...	(repeats)

Similarly, with j = 2, we obtain the third distinct null sequence C_3 of F(D) as :

C_1 :	11000,	....	(repeats)
D^2C_1 :	00110,	....	(repeats)
$C_2 = C_1 \oplus D^2C_1$:	11110,	....	(repeats)

The null sequences C_1, C_2, C_3 together describe all the $2^4 - 1$ nonzero states of the 4 - stage fsr corresponding to the given delay polynomial; and thus the set of sequences C_i (i = 1, 2, and d) constitutes the complete solution of F(D). Since the sequences C_1 , C_2 and C_3 are all of equal period and less than $2^n - 1$, the given polynomial must be irreducible and nonprimitive (modulo-2). Furthermore, here too,

the null sequence C_1 given by G(x) with initial state '0001' has this initial state in the sequence at the end of the cycle in its reverse order (C_1 : '11000', ...)

GROUP C : Factorable polynomials

Next, suppose that the given polynomial F(D) is factorable. In such a case, depending on the nature and degree of its factors, the polynomial F(D) exhibits several null sequences of different periods. However all these sequences can be evaluated as discussed below :

For this purpose, factorable polynomials are divided into two classes as under :

Class 1 : (a) Polynomials with factors that are nonrepeated primitive, modulo-2.

(b) Polynomials with factors that are repeated primitive, modulo-2

Class 2 : (a) Polynomials with factors that are non-repeated irreducible but nonprimitive, modulo-2.

(b) Polynomials with factors that are repeated irreducible but nonprimitive, modulo-2

Class 1(a) : Polynomials with nonrepeated primitive factors.

Let F(D) be an nth degree delay polynomial having only nonrepeated primitive factors. In mathematical terms, F(D) may be expressed as :

$$F(D) = \prod_{i=1}^{k} F_i(D) , \qquad \text{(mod-2 arithmetic)} \;\; .. \;\; (1.17)$$

where the factors $F_i(D)$, i = 1 to k, are all nonrepeated primitive.

Let the degree of the factor -

$F_1(D)$ be n_1

$F_2(D)$ be n_2

- - - - - - - - - -

- - - - - - - - - -

and $F_k(D)$ be n_k .

Denoting the periods of the null sequences associated with the factors $F_1(D)$, $F_2(D)$, ... , $F_k(D)$ by N_1, N_2, ... , N_k respectively, we can write :

$N_1 = 2^{n_1} - 1$ bits

$N_2 = 2^{n_2} - 1$ bits

- - - - - - - - -

- - - - - - - - -

and $N_k = 2^{n_k} - 1$ bits,

as the factors are all primitive (modulo-2).

It is evident that all the distinct null-sequence of the nth degree polynomial F(D) under question together describe the $2^n - 1$ different binary n - tuples. Now, this complete solution of F(D) may be thought of as a 'Vector-Space', of binary n-tuples. Since the polynomial is factorable, the sets of the n-tuples constituting the null sequences of its factors may then be understood as subvector-spaces S_i of the whole vector space S. Furthermore, it is not difficult to see that the subspaces S_i are disjoint and that together they compose the whole space S, as the factors are assumed to be relatively prime. Any cycle started in particular subspace must lie entirely within that subspace. Thus, the sequential behaviour of the fsr, governed by the polynomial F(D), over the whole space S may be described by considering its action seperately over each of the subspaces.

In view of the above concept, we may now introduce the following theorem, which facilitates the determination of all the null sequences associated with the delay polynomial under consideration.

Theorem 2 :

If F(D) is a binary nth degree delay polynomial and is the product of k factors denoted by $F_i(D)$, i = 1 to k, all of which

are nonrepeated primitive modulo-2, then, the following set of null sequences constitutes the complete solution of the polynomial F(D) :

(i) Null sequences of each of its factors, (These are in all k sequences), and

(ii) all possible sequences obtained by considering the modulo-2 sum of any q (q = 2 to k) of the k-sequences of its factors. The period of the so obtained sequence will be the L.C.M. of the various periods under consideration.

An example now follows.

Example 1.8 (A case of polynomial with nonrepeated primitive, modulo-2, factors.)

Consider the 5th degree delay polynomial given by :

$$F(D) = (I \oplus D^4 \oplus D^5)$$

It is desired to find all the null sequences of the polynomial.

Factorizing the polynomial and comparing with the general expression for F(D) stated in eqn. (1.17);

$$F(D) = (I \oplus D \oplus D^2) (I \oplus D \oplus D^3)$$

$$= F_1(D) \cdot F_2(D)$$

The polynomials, $F_1(D)$ of degree $n_1 = 2$ and $F_2(D)$ of degree $n_2 = 3$ respectively, are primitive modulo-2. (Table 1.5)

The null sequences, (say) C_1 and C_2, of the factors $F_1(D)$ and $F_2(D)$ can be determined from the generating function $G(x)$, given in eqn. (1.15) as under :

For $F_1(D)$: (Initial state of the corresponding fsr: 01)

$$G(x) = \left(\frac{I}{I \oplus D \oplus D^2} \right)$$

$$= (I \oplus D \oplus D^3 \oplus D^4 \oplus D^6 \oplus \ldots \text{ etc.})$$

Hence, the null sequence C_1 of $F_1(D)$ is :

C_1 : 110, 110, ... (repeats)

and is of period $N_1 = 2^{n_1} - 1 =$ 3 digits.

Similarly, for $F_2(D)$: (Initial state of the corresponding fsr; 001)

$$G(x) = \left(\frac{I}{I \oplus D \oplus D^3} \right)$$

$$= (I \oplus D \oplus D^2 \oplus D^4 \oplus D^7 \oplus D^8 \oplus D^9 \oplus D^{11} \oplus D^{14} \oplus \ldots\ldots \text{ etc. })$$

Hence, the null sequence C_2 of $F_2(D)$ is :

C_2 : 1110100, 1110100, ...(repeats)

and is of period $N_2 = 2^{n_2} - 1 = 7$ digits

Further, by theorem 2 (stated earlier), adding the sequences C_1 and C_2 in the modulo-2 sense, we obtain another null sequence, (say) C_3, of F(D) as :

C_1 : 11011011011011011011 .....

C_2 : 11101001110100111010 .....

$C_3 = C_1 \oplus C_2$: 00110010101111100010, ... (repeats)

and is of period $N_3 = N_1 N_2$ (L.C.M. of N_1 and N_2)

$= 21$ digits

The Σ length of the sequences C_1 , C_2 and C_3 of the 5th degree polynomial F(D) is :

$$N = (N_1 + N_2 + N_3) = 3 + 7 + 21$$

$$= 31 \ (= 2^5 - 1)$$

The sequences C_1 , C_2 and C_3 together describe all the $2^5 - 1$ binary n-tuples of the 5th degree polynomial F(D) and thus they together constitute its complete solution.

It is noteworthy here that the sequence C_3 exhibits certain noise features, which will be discussed later. Indeed any sequence obtained by modulo-2 sum of two or more m-sequences (over their common period) possesses certain noise-characteristics.

In the example cited above, the periods N_1 and N_2 of the sequences C_1 and C_2 respectively are relatively prime. In case N_1 and N_2 are not prime to each other, then the sequence obtained by modulo-2 addition of the sequences will be of period equal to L.C.M. of N_1 and N_2. In such a case, we obtain N_1 (or N_2) sequences of length N_2 (or N_1) digits, by applying theorem 2 stated earlier.

The results of a polynomial covering this situation are given below :

Example 1.9 : (A case of a polynomial having non-repeated primitive factors with periods not prime to each other)

$$F(D) = (I \oplus D^3 \oplus D^4 \oplus D^5 \oplus D^6)$$

$$= (I \oplus D \oplus D^2) (I \oplus D \oplus D^4)$$

$$= F_1(D) \cdot F_2(D)$$

The null sequences of the factors $F_1(D)$ and $F_2(D)$ are :

C_1 : 110, ... repeats, with period N_1 = 3 bits, and

C_2 ; 111101011001000, ... repeats, with period N_2 = 15 bits

Clearly, the periods N_1 and N_2 are not relatively prime. Applying theorem 2, we obtain the following null sequences (N_1 sequences of length N_2 digits since N_1 divides into N_2) of F(D) :

C_1	:	110110110110110	.... etc.
C_2	:	111101011001000,	.... etc.
$C_3 = C_1 \oplus C_2$	:	001011101111110,	.. (repeats) period N_3 = 15 bits
DC_1	:	011011011011011	.... etc.
C_2	:	111101011001000,	.... etc.
$C_4 = DC_1 \oplus C_2$	:	100110000010011,	.. (repeats) period N_4 = 15 bits
D^2C_1	:	101101101101101	.... etc.
C_2	:	111101011001000,	.... etc.
$C_5 = D^2C_1 \oplus C_2$	:	010000110100101,	.. (repeats) period N_5 = 15 bits

The length of the sequences C_1 to C_5 is :

$$N = N_1 + N_2 + N_1 (N_3 = N_4 = N_5)$$
$$= 3 + 15 + 3(15) = 2^6 - 1 \text{ bits}$$

Class 1(b) : Polynomial with repeated primitive factors.

Consider a delay polynomial $F(D)$, which is the product of repeated primitive factors expressed as :

$$F(D) = [F_1(D)]^{u_1} \cdot [F_2(D)]^{u_2} \ldots [F_k(D)]^{u_k}$$

$$= G_1(D) \cdot G_2(D) \ldots G_k(D) \quad \text{(say)} \quad \ldots (1.18)$$

Let the degree of the factor of $F(D)$

$F_1(D)$ be n_1

$F_2(D)$ be n_2

. . . . . .

. . . . . , and

$F_k(D)$ be n_k

Since the factors $F_i(D)$, $i = 1$ to k, are primitive, their null sequence periods N_i become :

$$N_i = 2^{n_i} - 1, \qquad i = 1 \text{ to } k.$$

To obtain all the null sequences of the original polynomial $F(D)$, it is at first necessary to find the null sequences of the individual terms $G_i(D)$, $i = 1$ to k. To this end, we may utilize the following theorem formulated by Golomb (1955).

Theorem 3 :

If $F_i(D)$ is a primitive (modulo-2) delay polynomial and $G_i(D) = [F_i(D)]^{u_i}$, the period λ_i of the null sequence of $G_i(D)$ is a multiple $e(u_i)$ of the period N_i of $F_i(D)$. That is, $\lambda_i = e(u_i)\, N_i$, where $e(u_i)$ is given by :

u_i	$e(u_i)$
1	1
2	2
3-4	4
5-8	8 .. etc.

From the knowledge of null sequences of the terms $F_i(D)$, the null sequences of the terms $G_i(D)$ are determined as shown below :

Consider the first term $G_1(D)$ -

$$G_1(D) = [F_1(D)]^{u_1} \quad .. \quad .. \quad .. \quad (1.19)$$

The degree of $F_1(D)$ being n_1, $G_1(D)$ is of degree $n_1^{u_1} = v_1$ (say). The null sequences of $G_1(D)$ together describe, thus in all $2^{v_1} - 1$ binary v_1-tuples. Therefore, the number of null sequences of $G_1(D)$ of period λ_1 digits is given by :

$$2^{v_1} - 1 = (N_1 + \lambda_1/\mu_1) \ , \ \mu_1 \text{ is an integer.... } (1.20)$$

Since, N_1, λ_1 and v_1 are known, μ_1 can be found.

Thus, with the help of theorem 3, and equn. (1.20), the period and number of null sequences of $G_1(D)$ can be known. However, the sequences are to be determined by means of the generating function G(x) and theorem 1.

Likewise, the null sequences of the rest of the terms $G_i(D)$ can be evaluated.

The following theorem is stated, which facilitates the evaluation of all null sequences of F(D) from the knowledge of null sequences of its terms $G_i(D)$, i = 1 to k.

Theorem 4 :

If F(D) is a binary delay polynomial expressed as :

$$F(D) = \prod_{i=1}^{k} G_i(D),$$

$$G_i(D) = [F_i(D)]^{u_i},$$

$F_i(D)$, i = 1 to k, being primitive modulo-2, and

if

G_{11} , G_{12} , ... etc. are the null sequences of $G_1(D)$,

G_{21} , G_{22} , ... etc. are the null sequences of $G_2(D)$,

. . . . .

. . . . .

G_{k1} , G_{k2} , ... etc. are the null sequences of $G_k(D)$,

then, the null sequences of the polynomial F(D) are :

(i) the null sequences of all the terms $G_i(D)$, i = 1 to k, and,

(ii) all possible sequences obtained by modulo-2 sum of two or more sequences of the different terms $G_i(D)$, i = 1 to k. The period of the sequence so obtained equals the L.C.M. of the periods of the different sequences that are modulo-2 added.

When two or more sequences have periods that are not relatively prime, the delay polynomial F(D) exhibits several shorter null sequences instead of a single long null sequence. An example now follows :

Example 1.10 : (A case of polynomial with repeated primitive factors.

Consider the delay polynomial given by :

$$F(D) = (I \oplus D^8 \oplus D^{10})$$

$$= (I \oplus D \oplus D^2)^2 (I \oplus D \oplus D^3)^2$$

It is desired to find all the null sequences of the polynomial.

Comparing the above polynomial with the general expression (1.18), we see that :

$G_1(D) = [F_1(D)]^{u_1}$, $F_1(D) = I \oplus D \oplus D^2$, and $u_1 = 2$.

$$G_2(D) = [F_2(D)]^{u_2}, \quad F_2(D) = I \oplus D \oplus D^3 \text{ and } u_2 = 2$$

Utilizing the generating function given in equation (1.14), the null sequences C_1 and C_2 of the factors $F_1(D)$ and $F_2(D)$, respectively, are seen to be :

C_1 : 110, 110, ... etc. ; period N_1 = 3 digits

C_2 : 1110100, 1110100, ... etc. period N_2 = 7 digits

By theorem 3, the period λ_1 of the null sequence of $G_1(D)$ is :

$$\lambda_1 = e(u_1)N_1$$
$$= (2)(3) = 6 \text{ digits}$$

From eqn. (1.20), the number of null sequences μ_1 of $G_1(D)$ with period λ_1 = 6 digits is given by

$$(2^{v_1} - 1) = N_1 + \mu_1 \lambda_1$$

where v_1 is the degree of $G_1(D)$.

Here, $v_1 = 4$, $N_1 = 3$, and $\lambda_1 = 6$

Therefore $\mu_1 = 2$

Likewise, the period of the null sequence of $G_2(D)$ is

$$\lambda_2 = e(u_2)N_2$$
$$= (2)(7) = 14 \text{ digits}$$

And, the number of null sequences μ_2 of $G_2(D)$ with period λ_2 equal to 14 digits is given by :

$$(2^{v_2} - 1) = N_2 + \mu_2 \lambda_2$$

where v_2 is the degree of $G_2(D)$

Here, $v_2 = 6$, $N_2 = 14$, and $\lambda_2 = 14$

Hence, $\mu_2 = 4$.

From the generating function G(x) of eqn.(1.14), the null sequence of the polynomial $G_1(D)$ with the initial state ' 0001 ' is :

G_{11} : 101000, ... (repeats)

and is of period $\lambda_1 = 6$ digits

As $\mu_1 = 2$, $G_1(D)$ has another null sequence G_{12} of period 6 digits. This can be obtained by theorem 1 as shown below :

G_{11} : 101000, ... (repeats)
DG_{11} : 010100, ... "

G_{12} : 111100, ... " (mod-2 sum of G_{11} and DG_{11})

Hence, the null sequences of the term $G_1(D)$ are :

(i) The sequence C_1 : 110, ... of period 3 bits,
(ii) The sequence G_{11}: 101000, ... of period 6 bits
(iii) The sequence G_{12}: 111100, ... of period 6 bits

And Σ length of all null sequences of the 4th degree term $G_1(D)$ is :

$$N_1 + \mu_1(\lambda_1) = 3 + 2(6)$$
$$= (2^4 - 1) \text{ bits}$$

In a similar manner, the null sequences of the term $G_2(D)$ may be evaluated as shown below :

The null sequence of $G_2(D)$ described by the generating function G(x) of eqn. (1.14) with initial state '000001' is :

G_{21} : 10101000100000, ... (repeats)

and is of period $\lambda_2 = 14$ bits

Since $\mu_2 = 4$, $G_2(D)$ has 3 more null sequences of period $\lambda_2 = 14$ digits. These are found by theorem 1 as :

G_{21} : 10101000100000, ... (repeats)
DG_{21} : 01010100010000, ... "

G_{22} : 11111100110000, ... " ($G_{22} = G_{21} \oplus DG_{21}$).

G_{21} : 10101000100000, ... (repeats)
D^3G_{21} : 00010101000100, ... "

G_{23} : 10111101100100, ... " ($G_{23} = G_{21} \oplus D^3G_{21}$).

G_{21} : 10101000100000 .... (repeats)

D^5G_{21} : 00000101010001,.... "

G_{24} : 10101101110001,.... " ($G_{24} = G_{21} \oplus D^5G_{21}$).

Thus, the null sequences of the 6th degree term $G_2(D)$ are :

(i) The sequence C_2 : 1110100, ... of period 7 bits,

(ii) The sequence G_{21}: 10101000100000, ... of period 14 bits,

(iii) The sequence G_{22}: 11111100110000, ... of period 14 bits,

(iv) The sequence G_{23}: 10111101100100, ... of period 14 bits,

(v) The sequence G_{24}: 10101101110001, ... of period 14 bits

And ∴ length of all null sequences of the 6th degree term $G_2(D)$ is :

$$N_2 + \mu_2(\lambda_2) = 7 + 4(14)$$

$$= (2^6 - 1) \text{ bits}$$

With the knowledge of the null sequences of the terms $G_1(D)$ and $G_2(D)$, we may now find the null sequences of the original polynomial F(D) by means of theorem 4 as follows :

By theorem 4, the null sequences of the polynomial F(D) are :

(i) The null sequences of the terms $G_1(D)$ and $G_2(D)$, and

(ii) The sequences obtained by modulo-2 sum of two or more null sequences of $G_1(D)$ and $G_2(D)$.

The complete solution to the polynomial F(D), obtained in accordance with theorem 4, is given in tabular form below :

Table 1.12 :

Null-sequence of F(D)	Succession of digits in the null sequence	Period in bits
C_1	110, ... etc.	3
C_2	1110100,.. etc.	7
G_{11}	101000, .. etc.	6
G_{12}	111100, .. etc.	6
G_{21}	10101000100000, ...	14
G_{22}	11111100110000, ...	14
G_{23}	10111101100100, ...	14
G_{24}	10101101110001, ...	14

(continued)

(Table 1.12 continued)

Null-sequence of F(D)	Succession of digits in the null sequence	Period in bits
$C_1 \oplus C_1$	(.., 0101111100001000110 01,...)	21
$C_1 \oplus G_{21}$	(.., 0111001111101111000 10 10011010001111001011 0,...)	42
$C_1 \oplus G_{22}$	(.., 0010011110101110010 00 10111010100101000021 0,...)	42
$C_1 \oplus G_{23}$	(.., 0110011011111111101 000 00010010000101101001 0,...)	42
$C_1 \oplus G_{24}$	(.., 0111011010101011000 00 00111000001101100011 1,...)	42
$G_{11} \oplus C_2$	(.., 0100101101011001100 01 11111101100000101112 0,...)	42
$G_{11} \oplus G_{21}$	(.., 0000101000001000100 01 01010101000000000100 0,...)	42
	and	
$G_{11} \oplus G_{21}$	(.., 1111011011001011011 11 00110100111111001110 00,...)	42
$G_{11} \oplus G_{22}$	(.., 0101111001001001110 11 01110101101010001100 0,...)	42
	and	
$G_{11} \oplus G_{22}$	(.., 1110100010010010101 10 11000011011100111010 1,...)	42

(continued)

(Table 1.12 continued)

Null-sequence of F(D)	Succession of digits in the null sequence	Period in bits
$G_{11} \oplus G_{23}$	(.., 000111110001100011011 11011101001010100 1100,..)	42
	and	
$G_{11} \oplus G_{23}$	(.., 111011001101011111100 01111111010100111 0000,..)	42
$G_{11} \oplus G_{24}$	(.., 000011110100110010011 11110111000010101 1001,..)	42
	and	
$G_{11} \oplus G_{24}$	(.., 111111001000001110100 01101001011100110 0101,..)	42
$G_{12} \oplus C_2$	(.., 000110100001110010011 01110111101010100 1000,..)	42
$G_{12} \oplus G_{21}$	(.., 010110110100110110011 11011111001010001 1100,..)	42
	and	
$G_{12} \oplus G_{21}$	(.., 110100010110010100111 10001110011011011 1110,..)	42
$G_{12} \oplus G_{22}$	(.., 000011110000110011001 11111111100000000 1100,..)	42
	and	
$G_{12} \oplus G_{22}$	(.., 100001010010010001101 10101110110001010 1110,..)	42

(continued)

(Table 1.12 continued)

Null-sequence of F(D)	Succession of digits in the null sequence	Period in bits
$G_{12} \oplus G_{23}$	(.., 0100111001011101110010101011100000001011000,..)	42
	and	
$G_{12} \oplus G_{23}$	(.., 1100010001110101011000000110010001111101 0,..)	42
$G_{12} \oplus G_{24}$	(.., 0101111000001001100010111110100100010011101,..)	42
	and	
$G_{12} \oplus G_{24}$	(.., 1101010000100001001010010110001100111011111,..)	42

Σ length of all distinct null sequences of the polynomial F(D) of degree n = 10 :

$$N = 3 + 7 + 2(6) + 4(14) + 21 + 22(42)$$

$$= 1023$$

$$= 2^{10} - 1$$

Class 2(a) : Polynomial with nonrepeated irreducible but nonprimitive factors (modulo-2) :

Let F(D) be an mth degree polynomial having only nonrepeated irreducible but nonprimitive factors. F(D) may be expressed as :

$$F(D) = \prod_{j=1}^{k} f_j(D)$$

where the factors $f_j(D)$ are all nonrepeated irreducible but nonprimitive factors.

Let the degree of the factor

$f_1(D)$ be m_1 ,

$f_2(D)$ be m_2 ,

. . . . . .

. . . . . .

and $f_k(D)$ be m_k .

Denoting the periods of the null sequences of the factors $f_1(D)$, $f_2(D)$ ...., $f_k(D)$ by M_1, M_2, ... , M_k, respectively, we can write that

$f_1(D)$ has a set of $\frac{2^{m_1} - 1}{M_1}$ cycles of period M_1, which may be represented by 'A_1' ,

$f_2(D)$ has a set of $\frac{2^{m_2} - 1}{M_2}$ cycles of period M_2, which may be represented by 'A_2',

. . . . . .

. . . . . .

and $f_k(D)$ has a set of $\frac{2^{m_k} - 1}{M_k}$ cycles of period M_k ; which may be represented by 'A_k', as the factors are all irreducible and nonprimitive, modulo-2.

It is evident that all the distinct null-sequences of the mth degree polynomial F(D) under question together must describe the $2^m - 1$ distinct binary m-tuples. Furthermore, all the null sequences should be derived from the null sequences of its factors. In view of the situation, the following theorem is presented which helps evaluate all the null sequences of the delay polynomial under consideration.

Theorem 5 :

If F(D) is a binary mth degree delay polynomial and is a product of k factors, denoted by $f_i(D)$, $i = 1$ to k, all of which are nonrepeated irreducible but nonprimitive modulo-2, then, the complete set of null-sequences of F(D) are :

(i) The sets of null sequences A_i, $i = 1$ to k, of period

$$\frac{2^{m_i} - 1}{M_i}$$

of all its factors, where m_i and M_i are the degrees and periods of the factors $f_i(D)$, and

(ii) All possible sequences obtained by modulo-2 sum of the null sequences belonging to the different sets of sequences A_i of its factors.

An example now follows.

Example 1.11 : (A case of polynomial with nonrepeated irreducible but nonprimitive factors).

Consider the delay polynomial given by :

$$F(D) = (I \oplus D^2 \oplus D^3 \oplus D^5 \oplus D^6 \oplus D^9 \oplus D^{10})$$

$$= (I \oplus D \oplus D^2 \oplus D^3 \oplus D^4) (I \oplus D \oplus D^2 \oplus D^4 \oplus D^6)$$

$$= f_1(D) \cdot f_2(D)$$

It is desired to find the null sequences of the polynomial F(D).

By means of the generating function G(x) of equation (1.15), with initial state '0001', one null sequence of m_1 = 4th degree factor $f_1(D)$ is :

C_{11} = 11000, ... (repeats)

and is of period M_1 = 5 digits.

Hence, there are in all $\frac{2^{m_1} - 1}{M_1}$ = 3 null sequences of period M_1 = 5 digits for $f_1(D)$, including sequence C_{11}. The other sequences, C_{12} and C_{13} (say) are found by Theorem 1 as written below :

$C_{12} = C_{11} \oplus DC_{11}$ = 10101, ... (repeats)

$C_{13} = C_{11} \oplus D^2C_{11}$ = 11110, ... (repeats)

Let the set of sequences (C_{11} , C_{12} , and C_{13}) be denoted by 'A_1'.

In a similar manner, the null sequences of the 6th degree factor $f_2(D)$ are determined and written below :

C_{21} = 11010011001001010000, ... (repeats)

C_{22} : 10111010101101111000, ... (repeats)

C_{23} : 11100111111010110001000, ... (repeats)

Let the set of sequences (C_{21}, C_{22}, and C_{23}) of period M_2 = 21 digits be denoted by 'A_2'.

Now by theorem 5, the null sequences of the original polynomial F(D) are :

(i) The sets of null sequences A_1 and A_2 , and

(ii) The sequences derived from modulo-2 summation of the null sequences belonging to the different sets A_1 and A_2 of its factors $f_1(D)$ and $f_2(D)$ respectively.

The complete solution, so obtained , is written below in in tabular form :

Null sequence of F(D)	Succession of digits in the null sequence	Period in bits
C_{11}	11000, ...	5
C_{12}	10101, ...	5
C_{13}	11110, ...	5
C_{21}	11010011001001010000, ...	21
C_{22}	10111010101101111000, ...	21
C_{23}	11100111111010110001000, ...	21

(continued)

Null sequence of F(D)	Succession of digits in the null sequence	Period in bits
$C_{11} \oplus C_{21}$	(.., 000101010001010010001 010111110100011000011 110010111110001100110 111000101010100101100 101100000011110111000,...)	105
$C_{11} \oplus C_{22}$	(.., 011111001000011000001 001101101101010010011 101000100111000110110 100010110011101111100 110110011010111101000,...)	105
$C_{11} \oplus C_{23}$	(.., 001000011101110111001 011010111000111101011 111111110010101001110 110101100110000000100 100001001111010010000,...)	105
$C_{12} \oplus C_{21}$	(.., 011111100100111001011 100010011111001110110 011001101000100001101 101110000111111111010 000001011001000010101,...)	105
$C_{12} \oplus C_{22}$	(.., 000101111101110011011 111000000110000100110 000011110001101011101 110100011110110101010 011011000000001000101,...)	105

(continued)

Null sequence of F(D)	Succession of digits in the null sequence	Period in bits
$C_{12} \oplus C_{23}$	(.., 010010101000011100011 101111010011101011110 010100100100000100101 100011001011011010010 001100010101100111101,..)	105
$C_{13} \oplus C_{21}$	(.., 001001001001100011101 001111000101111011011 000011011101001010111 011011101100101001111 101010001111101111110,..)	105
$C_{13} \oplus C_{22}$	(.., 010011011111101001101 010101011100110001011 011001000100000000111 000001110101100011111 110000010110100101110,..)	105
$C_{13} \oplus C_{23}$	(.., 000100000101000110101 000010001001011110011 001110010001101111111 010110100000001100111 100111000011001010110,..)	105

Σ length of all the distinct null sequences of the factorable polynomial F(D) is:

$$N = 3(5) + 3(21) + 9(105)$$
$$= 1023 \text{ bits}$$

Class 2(b) : Polynomial with repeated irreducible but nonprimitive factors (modulo-2)

Let F(D) be an mth degree delay polynomial having only repeated irreducible but nonprimitive factors (modulo-2) expressed as :

$$F(D) = [f_1(D)]^{u_1} \cdot [f_2(D)]^{u_2} \cdot\cdot [f_k(D)]^{u_k}$$

$$= h_1(D) \cdot h_2(D) \cdot\cdot h_k(D) \cdot\cdot \quad \cdot\cdot \quad \cdot\cdot \quad (1.21)$$

Eqn. (1.21) is similar to eqn. (1.18) except that in the present case the factors $f_i(D)$ (i = 1 to k) are nonprimitive. Hence theorem 4 can be utilized to find the null sequences of the polynomial F(D) stated in eqn.(1.21). The results of a polynomial belonging to this class are given below :

Example 1.12 : (A case of a polynomial with repeated irreducible but nonprimitive factors)

Consider the polynomial F(D) given by :

$$F(D) = (I \oplus D^2 \oplus D^4 \oplus D^6 \oplus D^8)$$

$$= (I \oplus D \oplus D^2 \oplus D^3 \oplus D^4)^2$$

$$= h_1(D) \quad \text{(say)}$$

It is desired to find the null sequences of F(D).

By means of the generating function G(x) of eqn.(1.15), one null sequence of $h_1(D)$ with initial state '00000001' is seen to be :

C_1 : 1010000000,... (repeats) and is of period M_1 = 10 bits.

The null sequences of $f_1(D) = (I \oplus D \oplus D^2 \oplus D^3 \oplus D^4)$ are: (already found in previous examples)

C_{11} : 11000,...

C_{12} : 10010,...

and C_{13} : 11110,...

By theorem 1 and repetitive application of the generating function, the complete solution of the original polynomial is determined and written below in tabular form :

Sr.No.	Null sequence of F(D)	Period in bits
1	(1000000010,..)	10
2	(1100000011,..)	10
3	(0010000010,..)	10
4	(1101000010,..)	10
5	(1010100010,..)	10
6	(1001010111,..)	10
7	(1000111110,..)	10
8	(1100100001,..)	10
9	(0010110001,..)	10
10	(0110011101,..)	10

(continued)

Sr.No.	Null sequence of F(D)	Period in bits
11	(1111111100,...)	10
12	(0110000011,...)	10
13	(0011000011,...)	10
14	(0111010011,...)	10
15	(1110001011,...)	10
16	(1010100111,...)	10
17	(1001100100,...)	10
18	(1011100011,...)	10
19	(0101011011,...)	10
20	(1111110110,...)	10
21	(0100101001,...)	10
22	(1101011001,...)	10
23	(0010011001,...)	10
24	(0001110111,...)	10
25	(10010,...)	5
26	(01111,...)	5
27	(11000,...)	5

Σ length of all distinct null sequences of the 8th degree polynomial F(D):

$$N = 24(10) + 3(5) = 255 \text{ bits}$$

1.6.2. Evaluation of null sequences of a delay polynomial by means of ' C_k - transform ' method

In the previous section, the generating function is made use of to obtain the null sequences of a given delay polynomial. It is also possible to find these sequences by ' C_k-transform method' as presented in this section. In fact, the C_k transform method is not radically different from the generating function approach. It just facilitates to derive a linear recurrence relation which the autonomous bistable feedback shift register satisfies.

Consider the characteristic equation (1.5) which is rewritten below :

$$\left[\oplus \sum_{i=0}^{n} a_i D^i \right] C = 0 \quad (\text{'}\oplus\text{' indicates mod-2 addition}) \qquad .. \quad (1.22)$$

i.e. $[F(D)] \quad C = 0$

where $F(D)$ is the delay polynomial, and where a_i represent the feedback coefficients of $F(D)$ having a value of either a 1 or 0, with $a_o = a_n = 1$.

To find the null sequences of the delay polynomial $F(D)$, we define a transform termed as 'C_k-transform', as :

$$\mathcal{C} \left[D^j C \right] = C_{k-j} \qquad .. \quad .. \quad (1.23)$$

where the symbol $\hat{C}$ stands for the transform of the jth delayed version of the variable C, and 'k and j' are integers.

Utilizing C_k-transform, the characteristic eqn.(1.5) may be written as :

$$C_k = a_1 C_{k+1} \oplus a_2 C_{k+2} \oplus \cdots \oplus C_{k+n} \quad .. \quad (1.24)$$

For this type of formulations, if the set of terms, $(C_{k+1}, C_{k+2}, \cdots, C_{k+1})$, may be thought of as representing the present state of the system, it is possible to ascertain the future states of the system by successive application of the expression (1.24). For instance, the immediate future state to the present state is given by the set of terms :

$$(C_k, C_{k+1}, C_{k+2}, \cdots, C_{k+n-1})$$

Likewise, it is possible to determine the past states of the fsr using C_k transform as follows :

Multiplying the characteristic equation by 'D' and applying C_k-transform:

$$C_{k+n+1} \oplus a_{n-1} C_{k+n} \oplus \cdots \oplus a_1 C_{k+2} = C_{k+1}$$

$$\text{i.e. } C_{k+n+1} = C_{k+1} \oplus a_1 C_{k+2} \oplus \cdots \oplus a_{n-1} C_{k+n} \quad .. \quad (1.25)$$

In accordance with eqn. (1.25), the immediate past state, is given by the set of terms $(c_{k+2}, c_{k+3}, \cdots, c_{k+n+1})$. And successively persuading the procedure, we can obtain all the past states of the fsr.

In brief, a linear recurrence, stated in eqn.s(1.24) and (1.25) may be utilized to evaluate null sequence(s) of a given delay polynomial. If the polynomial is primitive, for any nontrivial initial state, the sequence resulting from the above recursion algorithm will be of period $2^{n}-1$, where n is the degree of the polynomial. However, as pointed out in the previous sub-section, for irreducible but nonprimitive as well as factorable polynomial, many null sequences exist. To evaluate the complete set of null sequences, we may have to either repeat the above recursion algorithm with proper selection of initial states or resort to applying the theorems 1, 2, 3, 4 and 5 stated earlier(section 1.6.1). Since the application of these theorems is already clarified, only the use of C_k-transform to arrive at a null sequence for the three types of polynomials will now be illustrated.

Example 1.13 : A case of primitive polynomial).

Consider the delay polynomial given by :

$$F(D) = (I \oplus D \oplus D^3)$$

It is desired to find the null sequences of the polynomial by

the use of C_k-transform method.

The 3rd degree polynomial is primitive modulo-2 (Table 1.5).

The characteristic equation of the corresponding fsr is -

$$(I \oplus D \oplus D^3) C = 0$$

The C_k-transformed version of the above equation from expression (1.25) becomes :

$$c_{k+3} = c_k \oplus c_{k+1}$$

Considering the set of terms (c_1, c_2, c_3) as representing the initial state of the fsr, we may write all c_k's for $k > 3$ using the recursion formula (1.25), as follows :

With $k = 1$, $c_4 = c_1 \oplus c_2 = 0 \oplus 0 = 0$

$k = 2$, $c_5 = c_2 \oplus c_3 = 0 \oplus 1 = 1$

$k = 3$, $c_6 = c_3 \oplus c_4 = 1 \oplus 0 = 1$

$k = 4$, $c_7 = c_4 \oplus c_5 = 0 \oplus 1 = 1$

$k = 5$, $c_8 = c_5 \oplus c_6 = 1 \oplus 1 = 0$

$k = 6$, $c_9 = c_6 \oplus c_7 = 1 \oplus 1 = 0$

$k = 7$, $c_{10} = c_7 \oplus c_8 = 1 \oplus 0 = 1$

Since the last three c_ks (i.e. c_8, c_9 and c_{10}) represent the initial state '001', we stop persuading the recursion algorithm. The sequence consisting of the successive terms (c_1 , c_2 , ... , c_7 ; ... etc.) may be thought of as the

content of a virtual 7 stage system, governed by the characteristic equation :

$$(I \oplus D \oplus D^3) C = 0$$

The null sequence of the given polynomial is therefore :

$$C : \underset{\substack{| \\ c_7}}{1} \; \underset{\substack{| \\ c_6}}{1} \; 1 \; 0 \; 1 \; 0 \; \underset{\substack{| \\ c_1}}{0}, \ldots$$

where C now represents the input sequence to the 1st stage of the fsr.

We could have as well obtained this 'C' sequence using recursion formula given in eqn. (1.24). The next example, a case of irreducible but nonprimitive polynomial, illustrates the use of expression (1.24). Since the null sequence C obtained above describes all the distinct nonzero space of the given 3rd-degree binary fsr, we have obtained the complete solution for the given delay polynomial.

Example 1.14 : (A case of polynomial that is irreducible but nonprimitive, modulo-2).

Consider the delay polynomial given by :

$$F(D) = (I \oplus D \oplus D^2 \oplus D^3 \oplus D^4)$$

Find the null sequences of F(D).

The given polynomial is of degree 4 and is irreducible but nonprimitive, modulo-2 (Table 1.6).

The characteristic eqn. is :

$$(I \oplus D \oplus D^2 \oplus D^3 \oplus D^4)C = 0$$

The c_k- transformed version of the above equation from expression (1.24) is :

$$c_k = c_{k+1} \oplus c_{k+2} \oplus c_{k+3} \oplus c_{k+4}$$

Considering the set of terms (c_1 , c_2 , c_3 , c_4) as representing the initial state '0001' of the corresponding 4-stage fsr, we may write all c_ks for $k < 1$, using the recursion formula (1.24) as follows :

With $k = 0$, $c_o = c_1 \oplus c_2 \oplus c_3 \oplus c_4$

$= 0 \oplus 0 \oplus 0 \oplus 1$

$= 1$

$k = -1$, $c_{-1} = c_o \oplus c_1 \oplus c_2 \oplus c_3$

$= 1 \oplus 0 \oplus 0 \oplus 0$

$= 1$

$k = -2$, $c_{-2} = c_{-1} \oplus c_o \oplus c_1 \oplus c_2$

$= 1 \oplus 1 \oplus 0 \oplus 0$

$= 0$

$k = -3$ $c_{-3} = c_{-2} \oplus c_{-1} \oplus c_o \oplus c_1$

$= 0 \oplus 1 \oplus 1 \oplus 0$

$= 0$

$k = -4$ $c_{-4} = c_{-3} \oplus c_{-2} \oplus c_{-1} \oplus c_o$

$= 0 \oplus 0 \oplus 1 \oplus 1$

$= 0$

Since the set of terms (c_{-4} , c_{-3} , c_{-2} and c_{-1}) represent the initial state '0001', the algorithm need not be persuaded further.

The null sequence C, consisting of the terms (c_o , c_{-1} , c_{-2} , ... etc.) so obtained, reads as -

C_1 : 11000, ... (repeats)

With period $N_1 = 5 \ (< 2^4 - 1 = 15)$ digits. Clearly C_1 is not the only null sequence of the given polynomial. The other null sequences may be obtained by theorem 1 stated in Section 1.6.1.

In a similar manner, the C_k - transform can be made use of to find all null sequences of a factorable polynomial.

Thus, the generating function and the C_k-transform can be effectively applied to evaluate all the null sequences of a delay polynomial, together with the theorems 1, 2, 3, 4 and 5.

1.7 DETERMINATION OF DELAY POLYNOMIAL FROM ITS NULL SEQUENCE

This section deals with the determination of delay polynomials from its null sequence, which need not be maximal. Three methods have been introduced here for this purpose. In

the first method, the polynomial is determined by mere examination of the given sequence. This is hence called as'direct method'. The second method utilizes the relation between the generating function and delay polynomial associated with the sequence. Lastly, the third method is based on the C_k-transform and the linear recurrence developed in the last section.

1.7.1 Determination of delay polynomial by direct method

Let C, represented by the successive terms $(c_1, c_2, \ldots c_r)$, be the null sequence of period N, associated with a linear binary nth degree delay polynomial F(D), whereby $[F(D)]\ C = 0$ represents the characteristic equation of the corresponding autonomous fsr. To find F(D) corresponding to the given sequence C, we may proceed as follows :

Consider two consecutive states of the fsr such that in the first state (say reference state), all binary digits except one are zero. Let c' be the 1st binary digit in the immediate next state as depicted below :

	Stage Number							
	1	2	...	i	i + 1	...	n - 1	n
Reference state	0	0	...	c_i	0	...	0	0
Next state	c'	0	...	0	c_i	...	0	0

Now, c' is the modulo-2 sum of the contents of several of the stages at the 1st state. We may, therefore, write the following equation in this case :

$$c' = a_i c_i \qquad .. \qquad .. \qquad .. \qquad (1.26)$$

where a_i is the coefficient of D^i in the delay polynomial F(D), written as :

$$F(D) = \oplus \sum_{i=0}^{n} a_i D^i$$

(For the binary nth degree fsr, $a_o = a_n = 1$)

Since c' and c_i are known from the given sequence, the coefficient a_i may be found. Thus, by considering (n - 1) pairs of such consecutive states, it is possible to evaluate all the coefficients a_1 to a_{n-1} of the required polynomial F(D).

Evidently, the method assumes the occurance of n states in the given sequence C, in which all digits except one are zero. This limitation poses no problem in case the sequence is of maximum length. In fact, every binary m-sequence exhibits n such states.

The method is not applicable to nonmaximal sequences as these do not describe the required n states. In such a situation

either the generating function method or the C_k-transform method may be made use of as discussed in Sections(1.7.2) and(1.7.3) respectively.

An example by direct method now follows :

Example 1.15 : (A case of m-sequence)

Consider the binary m-sequence C given by :

C : 111101011001000, ... (repeats)

It is desired to find the delay polynomial F(D) that corresponds to the m-sequence C.

The given m-sequence is of period N = 15 digits and describes all the $2^4 - 1$ nontrivial states of a 4 stage fsr. Hence, the corresponding delay polynomial may be expressed as :

$$F(D) = (I \oplus a_1 D \oplus a_2 D^2 \oplus a_3 D^3 \oplus D^4)$$

(since $a_o = a_4 = 1$)

To determine the coefficients a_1 , a_2 and a_3 of F(D), the following states are considered :

For a_1 :

	Stage number of fsr			
	1	2	3	4
Reference state	1	0	0	0
Next state (read from sequence-C)	1	1	0	0

Making use of eqn. (1.26) :

$$1 = (a_1)(1)$$

Hence, $a_1 = 1$

For a_2 :

	Stage number of fsr			
	1	2	3	4
Reference state	0	1	0	0
Next state (read from sequence C)	0	0	1	0

Utilizing eqn. (1.26) :

$$0 = (a_2)(1)$$

Hence, $a_2 = 0$

For a_3 :

	Stage number of fsr			
	1	2	3	4
Reference state	0	0	1	0
Next state (read from sequence C)	0	0	0	1

Again from eqn. (1.26) :

$$0 = (a_3)(1)$$

Therefore, $a_3 = 0$

The delay polynomial corresponding to the given binary m-sequence C of period 15 digits is thus :

$$F(D) = (I \oplus D \oplus D^4)$$

The above result may be verified as under :

C : 111101011001000, ...

DC : 011110101100100, ...

D^4C : 100011110101100, ...

$(I \oplus D \oplus D^4)C$: All zero sequence

1.7.2 Use of 'Generating Function' in determining the delay polynomial from its null sequence

Let C, represented by the successive terms, $(c_1, c_2, \ldots c_r)$, be the given null sequence of period N, associated with a linear binary nth degree delay polynomial F(D), whereby $[F(D)]\ C = 0$ is the characteristic equation of the corresponding autonomous feedback shift register.

From the analysis of section (1.6.1), the generating function G(x) associated with the sequence C may be written in terms of the polynomial F(D) as (eqn. 1.14) :

$$G(x) = \frac{(\oplus_{i=0}^{n-1} b_i D^i)}{F(D)}\ x \quad \ldots\ \ldots\ \ldots \quad (1.14)$$
(repeated here)

which, for the initial state of '00...1', becomes :

$$G(x) = \frac{1}{F(D)}\ x \quad \ldots\ \ldots\ \ldots \quad (1.15)$$
(repeated here)

Further, it has been pointed in Section (1.6.1) that each cycle of the null sequence of the polynomial as described by the generating function G(x) starts with '1' and ends with the assumed initial state appearing in the reverse order (i.e. 000.01 as 10.000). In brief, each cycle of the sequence C starts with 1 and ends with (n-1) zeros for the assumed initial state '00...1'. Thus, we may find the polynomial F(D) from its null sequence C from equation (1.15) where G(x) is now written after arranging the given null sequence C such that it ends with a 1 followed by (n - 1) zeros. The method is applicable to maximal and nonmaximal sequences as detailed in the following examples. At times, the given sequence may not contain the required n-1 zeros. Such special cases are also considered below through examples.(Examples 1.17 and 1.18)

Example 1.16 : (A case of m-sequence)

Given the maximal length sequence C as :

C : 111100010011010, ... (repeats)

Find the corresponding delay polynomial F(D).

The period of the given binary sequence is 15 digits. Further, the sequence describes all the possible nonzero states of a 4-stage feedback shift register. Hence the delay polynomial of degree 4 may be expressed as :

$$F(D) = (I \oplus a_1 D \oplus a_2 D^2 \oplus a_3 D^3 \oplus D^4)$$

Arranging the sequence C such that each cycle of it ends with a 1 followed by (n - 1) zeros, C appears as :

C : 100110101111000, ... (repeats)

Since the sequence is cyclic, we need to consider only one period to determine the polynomial that corresponds to it.

The generating function for the single cycle considered, $G_1(x)$ reads from eqn. (1.15) as :

$$G_1(x) = \frac{I}{[F(D)]\, x}$$

$$\text{or } [F(D)]\; x = \frac{I}{G_1(x)}$$

$$= \left(\frac{I}{I \oplus D^3 \oplus D^4 \oplus D^6 \oplus D^8 \oplus D^9 \oplus D^{10} \oplus D^{11}}\right) x$$

$$= (I \oplus D^3 \oplus D^4)\, x \qquad \text{(by long division)}$$

Thus, the required polynomial is :

$$F(D) = (I \oplus D^3 \oplus D^4)$$

To check the results, it may be verified that

$$[F(D)]\; C = 0$$

Example 1.17 : (A case of nonmaximal length sequence)

Consider the null sequence given by :

C : 10100 ,... (repeats)

for which it is required to find the corresponding delay polynomial F(D).

The period of the given binary sequence is 5 digits. This means, it is a nonmaximal length sequence, since $2^n - 1 \neq 5$ for any n. Further, for $n \leq 3$, the possible longest nonmaximal sequence is of period 4 digits. Hence, the minimum value of the degree of F(D) corresponding to the given null sequence C should be 4.

Hence, F(D) may be written as :

$$F(D) = (I \oplus a_1 D \oplus a_2 D^2 \oplus a_3 D^3 \oplus D^4)$$

However, with this information, we cannot proceed further to determine the polynomial because the null sequence C does not have n - 1 = 3 zeros as required by the present method. To make the current method applicable, we now utilize the theorem 1 stated in section (1.6.1), which states that: if

If C is a null sequence of period N of a delay polynomial F(D), then, the sequences C_j described by

$$C_j = C \oplus D^j C , \qquad 1 \leq j < N$$

are also null sequences of the polynomial F(D).

Hence, with j=2, we get another null sequence (say) C_1 of the polynomial F(D) as under :

C :	10100, ...	(repeats)
D^2C :	00101, ...	(")
$C_1 = C \oplus D^2C$:	10001, ...	(")

Since both C and C_1 are the null sequences of the required polynomial F(D), and that the sequence C_1 contains n-1 = 3 zeros, we may rearrange it in accordance with the requirements of the present method, and find the corresponding polynomial F(D) as follows :

Original sequence C :	10100,...	(repeats)
Arranged sequence C_1 :	11000,...	(")

Now, considering a cycle of the arranged sequence C_1, the corresponding generating function $G_1(x)$ may be written as :

$$G_1(x) = (I \oplus D)$$

Making use of eqn. (1.15), and recalling that the desired polynomial F(D) is of degree 4, we get -

$$[F(D)]\ x = \left(\frac{I}{I \oplus D} \right) x$$

$$= (I \oplus D \oplus D^2 \oplus D^3 \oplus D^4)\ x$$

Thus, $F(D) = (I \oplus D \oplus D^2 \oplus D^3 \oplus D^4)$.

Example 1.18 : (A special case of nonmaximal length sequence)

Given the null sequence C as -

C : 10100101,... (repeats)

It is required to find the corresponding delay polynomial F(D).

Here, the given binary sequence is of period 8 digits and hence is nonmaximal because $8 \neq 2^n - 1$ for any n. Further the degree of the required polynomial should be atleast 5 (i.e. n = 5) since for $n \leq 4$, the longest nonmaximal sequence is of period 7 digits only.

Further, in this case, any permissible value of j in theorem 1 will not yield a null sequence of F(D) with n - 1 = 4 zeros. However, we can still solve the problem with the help of the general expression for the generating function stated in eqn. (1.14) and repeated below for convenience -

$$G(x) = \left(\frac{\sum_{i=0}^{n-1} b_1 D^i}{F(D)} \right)$$

$$= \left(\frac{F_1(x)}{F(x)} \right) \quad \text{(say)}$$

Here $F_1(x)$ is of degree $\leq n - 1$ and F(x) is of degree n. Hence, we may write :

$$G(x) = d_o \oplus d_1 x \oplus d_2 x^2 \oplus \ldots \oplus d_r x^r \oplus \ldots \text{ etc.}$$

Considering only one cycle of the null sequence, the generating function $G_1(x)$, therefore, is :

$$G_1(x) = d_o \oplus d_1 x \oplus d_2 x^2 \oplus \ldots \oplus d_{N-1} x^{N-1}, \quad \ldots (1.27)$$

where N is the period of the given null sequence.

Expanding eqn. (1.14), we see that -

$$d_o = b_o = \oplus \sum_{i=1}^{n} a_i c_{-i} ,$$

$$d_1 = b_1 \oplus b_o a_1 = \oplus \sum_{i=1}^{n-1} a_{i+1} c_{-i} \oplus a_1 \sum_{i=1}^{n} a_i c_{-i} ,$$

$$d_2 = b_2 \oplus b_1 a_1 \oplus b_o (a_2 \oplus a_1^2) ,$$

. . . . . .

. . . . . .

and $d_r = b_r \oplus \sum_{i=0}^{r-1} a_{r-i} d_i$ where $d_o = b_o$.

With the help of eqn. (1.27), we now proceed to solve the present example -

Sequence given : 10100101,...

Writing the generating function $G_1(x)$ of the sequence for one period :

$$G_1(x) = (I \oplus x^2 \oplus x^5 \oplus x^7) \quad \ldots \quad \ldots (1.28)$$

Comparing eqns. (1.27) and (1.28), we see that -

$$d_o = d_2 = d_5 = d_7 = 1,$$

and $d_1 = d_3 = d_4 = d_6 = 0$

As already pointed out, the null sequence given by G(x) ends with the initial state in the reverse order. Thus, the initial state in this case is as shown below -

$$C : 1\ 0\ 1\ \underset{|}{0}\ \underset{|}{0}\ 1\ 0\ \underset{|}{1}, \ldots$$
$$c_{-5}\ c_{-4} \cdots c_{-1}$$

Now,

$$d_o = \oplus \sum_{i=1}^{5} a_i c_{-i} = 1$$

i.e. $a_1 c_{-1} \oplus a_3 c_{-3} = 1$

Hence, $a_1 \oplus a_3 = 1$ ..... (i)

Nextly,

$$d_1 = \oplus \sum_{i=1}^{5-1} a_{i+1}\, c_{-i} \oplus a_1 \sum_{i=1}^{5} a_i c_{-i} = 0$$

On simplification, the above equation leads to :

$$a_2 \oplus a_4 = a_1 \quad \ldots\ldots\ldots \quad (ii)$$

Similarly,

$$d_2 = \oplus \sum_{i=1}^{5-2} a_{i+2} c_{-i} \oplus a_1 \sum_{i=1}^{5-1} a_{i+1} c_{-i} \oplus (a_2 \oplus a_1) \sum_{i=1}^{5} a_i c_{-i} = 1$$

from which we get, $a_2 \oplus a_3 \oplus a_5 = 1.$ ..... (iii)

From eqns. ((i), (ii) and (iii), the values of the feedback coefficients of the required delay polynomial are determined and written below :

(i) $a_1 = a_4 = 1$, and $a_2 = a_3 = 0$

OR

(ii) $a_2 = a_3 = a_4 = 1$, and $a_1 = 0$.

However, the condition (ii) is seen not to satisfy the equation :

$[F(D)]\, C = 0$, where C is the given sequence.

Hence, the polynomial F(D) corresponding to the given null sequence is :

$$F(D) = (I \oplus D \oplus D^4 \oplus D^5)$$

It may be verified that -

$$[F(D)]\, C = (I \oplus D \oplus D^4 \oplus D^5) C = 0.$$

Thus, by means of the generating function concept, it is possible to determine the delay polynomial from its null sequence, no matter whether the given sequence is of maximum length or otherwise.

1.7.3. C_k-transform and its use in determining the delay polynomial from its null-sequence

This sub-section is meant to develop the procedure for finding the delay polynomial from its null sequence making use of C_k-transform and associated linear recurrence stated earlier.

Let C, represented by the successive terms $(c_1, c_2, \ldots c_r)$, be the given null sequence of period N, associated with a linear binary nth degree delay polynomial F(D), whereby $[F(D)]\,C = 0$ stands for the characteristic equation of the corresponding autonomous linear fsr.

From the analysis of section (1.6.2), the C_k-transformed version of the characteristic equation (1.5) may be written in either of the forms stated below(linear recurrence relationship given in eqns. (1.24) and (1.25).)

$$c_k = a_1 c_{k+1} \oplus a_2 c_{k+2} \oplus \ldots \oplus c_{k+n}, \ldots \qquad (1.24)$$

$$c_{k+n+1} = a_o c_{k+1} \oplus a_1 c_{k+2} \oplus \ldots \oplus a_{n-1} c_{k+n} \qquad (1.25)$$

(repeated here)

Further, it is seen that for this type of formulation, if the set of terms $(c_{k+1}, c_{k+2}, \ldots, c_{k+n})$ represents the present state, then, it is possible to formulate both past

and future states of the fsr with the help of the above recursion formulae. To find the polynomial F(D) corresponding to the given null sequence, we may therefore consider (n-1) states of the fsr, and write the corresponding (n-1) equations with the help of either eqn. (1.24) or (1.25). Since the states are known, the feedback coefficients a_1 to a_{n-1} can be evaluated. ($a_o = a_n = 1$). The following example illustrates the technic of finding the delay polynomial from its null sequence by means of e_k-transform and the linear recurrence.

Example 1.19 : (A case of maximum length sequence)

Given the null sequence C as -

C : 1000011100110111110100010010101,... (repeats)

it is required to find the corresponding delay polynomial F(D).

The period of the given binary sequence is 31 digits. Further, the sequence C describes all possible non-zero states of a 5-stage fsr. Hence the corresponding delay polynomial, which is maximal, should be of degree 5, and may be written as :

$$F(D) = (I \oplus a_1 D \oplus a_2 D^2 \oplus a_3 D^3 \oplus a_4 D^4 \oplus D^5)$$

Hence, the characteristic equation of the corresponding linear shift register is :

$$[F(D)]\, C = (I \oplus a_1 D \oplus a_2 D^2 \oplus a_3 D^3 \oplus a_4 D^4 \oplus D^5)C = 0$$

The C_k-transformed version of the above characteristic equation is :

$$c_k = a_1c_{k+1} \oplus a_2c_{k+2} \oplus a_3c_{k+3} \oplus a_4c_{k+4} \oplus c_{k+5}$$

If c_1 , c_2 , c_3 , c_4 and c_5 (i.e. c_{k+1} , c_{k+2} , $\cdots c_{k+5}$ with $k = 0$) represent the present state of the fsr, then the following equations may be written :

$$c_o = a_1c_1 \oplus a_2c_2 \oplus a_3c_3 \oplus a_4c_4 \oplus c_5$$

$$c_{-1} = a_1c_o \oplus a_2c_1 \oplus a_3c_2 \oplus a_4c_3 \oplus c_4$$

$$c_{-2} = a_1c_{-1} \oplus a_2c_0 \oplus a_3c_1 \oplus a_4c_2 \oplus c_3$$

$$c_{-3} = a_1c_{-2} \oplus a_2c_{-1} \oplus a_3c_0 \oplus a_4c_1 \oplus c_2$$

If the initial state is considered as (arbitrarily chosen)

$c_1 = c_2 = c_3 = c_4 = 0$ and $c_5 = 1$,

then, from the given null sequence we see that :

$c_o = 1$, $c_{-1} = 1$, $c_{-2} = 1$, $c_{-3} = 0$, etc.

Substituting these values in the above eqns. and solving for the feedback coefficient, we obtain -

$a_1 = a_2 = a_4 = 1$ and $a_3 = 0$

Hence, the delay polynomial that corresponds to the given null sequence C is :

$$F(D) = (I \oplus D \oplus D^2 \oplus D^4 \oplus D^5)$$

Example 1.20 : (A case of nonmaximal sequence)

Given the null sequence C as :

C : 10000111110101001100 0,... (repeats)

find the corresponding delay polynomial.

The given binary sequence is of period 21 digits. This means that the sequence C is nonmaximal, since $2^n - 1 \neq 21$ for any n. Further, the fact that the period of the longest nonmaximal sequence realizable from an fsr of degree ≤ 4 is 7 digits, implies that the polynomial corresponding to the given sequence C should be at least of degree 5, and may be expressed as :

$$F(D) = (I \oplus a_1 D \oplus a_2 D^2 \oplus a_3 D^3 \oplus a_4 D^4 \oplus D^5)$$

As shown in the initial state (contained in given null sequence) as -

$$c_1 = c_2 = c_3 = c_4 = 0, \quad \text{and} \quad c_5 = 1,$$

the binary values of the terms c_o, c_{-1}, c_{-2} and c_{-3} may be read from the given sequence as -

$$c_o = c_{-1} = c_{-2} = c_{-3} = 1.$$

Further, the following equations for the above

terms can be written by means of the linear recurrence stated in eqn. (1.24) - (on substituting for terms c_1 to c_5)

$$c_o = c_5 = 1$$

$$c_{-1} = a_1 = 1$$

$$c_{-2} = a_1 \oplus a_2 = 1$$

$$c_{-3} = a_1 \oplus a_2 \oplus a_3 = 1$$

Solving for the feedback coefficients, we obtain

$$a_1 = 1, \text{and } a_2 = a_3 = a_4 = 0.$$

Therefore, the delay polynomial that corresponds to the given sequence C is -

$$F(D) = (I \oplus D \oplus D^5)$$

To check the result, it may be verified that :

$$[F(D)]\ C = (I \oplus D \oplus D^5)C = 0$$

The C_k-transform and associated linear recurrence is thus seen to be quite a convenient tool to solve such problems. It should be noted here that the method is applicable only when the given null sequence contains at least 2n - 1 digits, since n digits are needed as an initial condition and (n-1) additional digits are necessary to specify uniquely which of the stages of the corresponding fsr are to be fedback besides the nth stage which is always fedback.

1.8 PROPERTIES OF DELAY POLYNOMIALS AND THEIR NULL SEQUENCES

From the results of the analysis of sequential behaviour of autonomous linear binary feedback shift register so far carried out in this chapter, and what appears in the literature in somewhat scattered and disjointed form (the pertinent references are already stated in the introduction of the present chapter), useful properties of the characteristic delay polynomials and their null sequences are given in this section.

Here, as previously stated, F(D) is the characteristic binary delay polynomial of degree n as defined by eqn.(1.6), and C is its null sequence of period N in digits satisfying the relationship :

$$[F(D)]\ C = 0,$$

which is the characteristic equation of the corresponding autonomous linear binary feedback shift register.

1. Characteristic delay polynomials of several types exist for the positive modulus p = 2, and these may be classified, based on their factorable features (modulo-2) as -

(A) Irreducible and primitive polynomials
(B) Irreducible and nonprimitive polynomials
(C) Factorable polynomials.

2. Every delay polynomial has a complete set of distinct solutions or null sequences.

3. The period of the null sequence N of a delay polynomial F(D) is the smallest integer for which $I \oplus D^N$ is divisible by F(D).

Example :

$F(D) = I \oplus D^2 \oplus D^4$

$$
\begin{array}{l}
I \oplus D^2 \oplus D^4 \;\big)\; I \oplus D^N \;(\; I \oplus D^2 \\
\qquad\qquad\qquad\qquad\quad \underline{I \oplus D^2 \oplus D^4} \\
\qquad\qquad\qquad\qquad\qquad\quad D^2 \oplus D^4 \oplus D^N \\
\qquad\qquad\qquad\qquad\qquad\quad \underline{D^2 \oplus D^4 \oplus D^6} \\
\qquad\qquad\qquad\qquad\qquad\qquad\quad D^6 \oplus D^N
\end{array}
$$

If N = 6, the remainder of this division equals 0 ; hence 6 is the period of $F(D) = I \oplus D^2 \oplus D^4$.

4. A polynomial F(D), with coefficients in Galois Field GF(p = 2), (p is a prime integer), is irreducible and primitive over GF(p = 2) if the smallest nonzero integer N such that F(D) divides $I \oplus D^N$ is $N = 2^n - 1$, where n is the degree of F(D). The division is performed modulo-2.

Thus, an irreducible and primitive polynomial means that :

(i) The polynomial has no factor (modulo-2),

(ii) The polynomial (of degree n) is not a factor of $D^N \oplus 1$ for any integer $N < 2^n - 1$.

The statement implies that an irreducible and primitive polynomial of degree n has only one null sequence of period $2^n - 1$ digits, and the $2^n - 1$ nonzero binary n-tuples appear in this sequence before it repeats. Since the largest possible period for a linear binary n-stage fsr is $2^n - 1$, the null sequence of the primitive polynomial is called 'maximum length null sequence (mlns)'.

Accordingly, the irreducible and primitive polynomial is also called 'maximal polynomial'.

5. A polynomial is irreducible but nonprimitive (modulo-2) means that :

(i) The polynomial has no factors, but

(ii) The polynomial is a factor of $D^N \oplus 1$ for some integer $N < 2^n - 1$, (n is the degree of F(D).)

This statement and property (3) imply that an irreducible but nonprimitive polynomial has several null sequences, each of which is of period less than the maximum of $2^n - 1$ digits. These sequences are hence called nonmaximal null sequences.

However, the irreducibility of the polynomial insures that all its null sequences be of the same period.

6. The factorable polynomial (mod.2) is one that is reducible into two or more irreducible polynomials. The period and number of null sequences of a factorable polynomial depend on the nature and degrees of its factors. The null sequence of the factorable polynomial could even be of period less than the degree of the polynomial.

7. From properties (3), (4), (5) and (6), it follows that:

(i) The null sequence of the binary polynomial, irrespective of the class to which it belongs, is of period $N \leq 2^n-1$.

(ii) The necessary, but insufficient, condition that the period of the null sequence of a polynomial of degree n to be 2^n-1 digits is that the polynomial be irreducible.

(iii) Every maximal polynomial is necessarily irreducible, but every irreducible polynomial is not maximal.

8. For every polynomial, the $\leq$ periods of its distinct null sequences equal 2^n-1 digits.

9. If the two states of an m-sequence are +1 and -1, then the number of zero crossings is 2^{n-1}.

10. For an n-stage fsr, there are exactly $\phi(2^n - 1) / n$ maximal polynomials, where $\phi(k)$ is the Euler's phi function and is defined as the number of positive integers less than k, and relatively prime to k including 1.

This statement is proved by Zierler (1959) who shows that since the characteristic polynomial of an m-sequence must be a minimum polynomial of a primitive $(N = 2^n-1)$th root of unity, and since there are exactly $\phi(2^n-1) / n$ different equations of degree n that are minimum equations of primitive Nth root of unity, the above statement must be true.

Example :

Let n be equal to 7. We wish to find the value of $\phi(2^7 - 1) = \phi(127)$. Since every integer less than 127 is relatively prime to 127, there are 126 integers less than and prime to 127. Therefore, $\phi(127) = 126$. Dividing this by 7, shows that there are 18 maximal polynomials for n = 7 (This may be verified from Table 1.5).

The integer $\phi(k)$ may be calculated, depending upon whether k contains factors or is prime. If k is factorable, then , $\phi(k) = k \cdot (Q_i - 1) / Q_i$, where Q_i are the prime factors of k. If k is a prime number, then $\phi(k) = k - 1$.

11. No delay polynomial having even number of feedback coefficients of value 1 (excluding a_n, which is always unity for the binary n-stage fsr) can produce an m-sequence.

This becomes obvious if the polynomial is solved for its null sequence with an 'all-1' initial state. With an even number of feedback coefficients, the digit fedback will always be 1, so that the resulting sequence will be all ones with a period of one. As the Σ periods of all distinct sequences of the polynomial must be 2^n-1, the longest sequence is atmost (2^n-2). Hence the statement is true.

12. For every n, there exist two maximal polynomials, which possess null sequences that are time-reverse of each other. The reverse sequence the original sequence read in the reverse order.

If an n-stage fsr has feedback connections from stages n, k, m,.. etc., the reverse sequence fsr will have feedback connections from stages n, n - k, n - m, etc.

13. For every polynomial of degree n, its null sequence C satisfies a linear recurrence relation :

$$c_r = \bigoplus_{i=1}^{n} a_i c_{r-i}$$

where c_r is any term in the sequence c, and a_i, the coefficients of the polynomial having a value of either a 1 or a 0. ($a_n = 1$).

14. By means of the above linear recurrence; given a polynomial, it is possible to evaluate all its null sequences. Alternatively, given a null sequence realizable from an fsr of degree n, the corresponding delay polynomial can be found using the linear recurrence relation.

15. Every null sequence C, represented by the terms $(c_o , c_1, \ldots, c_r \ldots)$ may be expressed by the associated generating function as -

$$G(x) = \sum_{r=0}^{\infty} c_r x^r = \oplus \left(\frac{\sum_{i=0}^{n-1} b_i D^i}{F(D)} \right) x$$

where $b_j = \oplus \sum_{i=1}^{n-i} a_{i+j} c_{-i}$

16. Given a delay polynomial and the initial state, all its null sequences can be evaluated with the help of the generating function concept. Likewise, the delay polynomial corresponding to a given null sequence can be determined.

17. The null sequence of a polynomial as given by the generating function G(x) always ends with the presumed initial stage appearing in its reverse order.

18. The linear recurrence relation stated under property 13 leads to the concept of vector diagram, that can be used to describe the sequential behaviour of the linear shift register, as outlined below :

18. The linear recurrence relation indicates that an n-stage fsr can be described as a device which takes any input vector (c_1 , c_2 , ..., c_n) and computes an output vector (c_o, c_1, ... c_{n-1}). Hence, the sequential behaviour of any linear fsr can always be represented by means of a vector diagram showing all possible input and output vectors.

Such a vector diagram for the case of linear recurrence given by -

$$c_r = c_{r-1} \oplus c_{r-2} \oplus c_{r-3} \oplus c_{r-4}$$

is depicted in Fig. 1.7.

With reference to this vector diagram, the following conditions are equivalent :

1(i) Cycles in the vector diagram have no branch points.

(ii) Every vector has a predecessor as well as a successor.

(iii) Predecessors of vectors, when they exist, are unique.

(iv) Distinct vectors have distinct successors.

(v) The feedback relation $c_r = F(c_{r-1}, \ldots, c_{r-n})$ can be decomposed into :

$$F(c_{r-1}, \ldots, c_{r-n+1}) \oplus c_{r-n}$$

19. If $C = (c_o , c_1 , c_2 , \ldots)$ is a null sequence, which need not be maximal, of period N associated with a delay polynomial, then, the sequences given by :

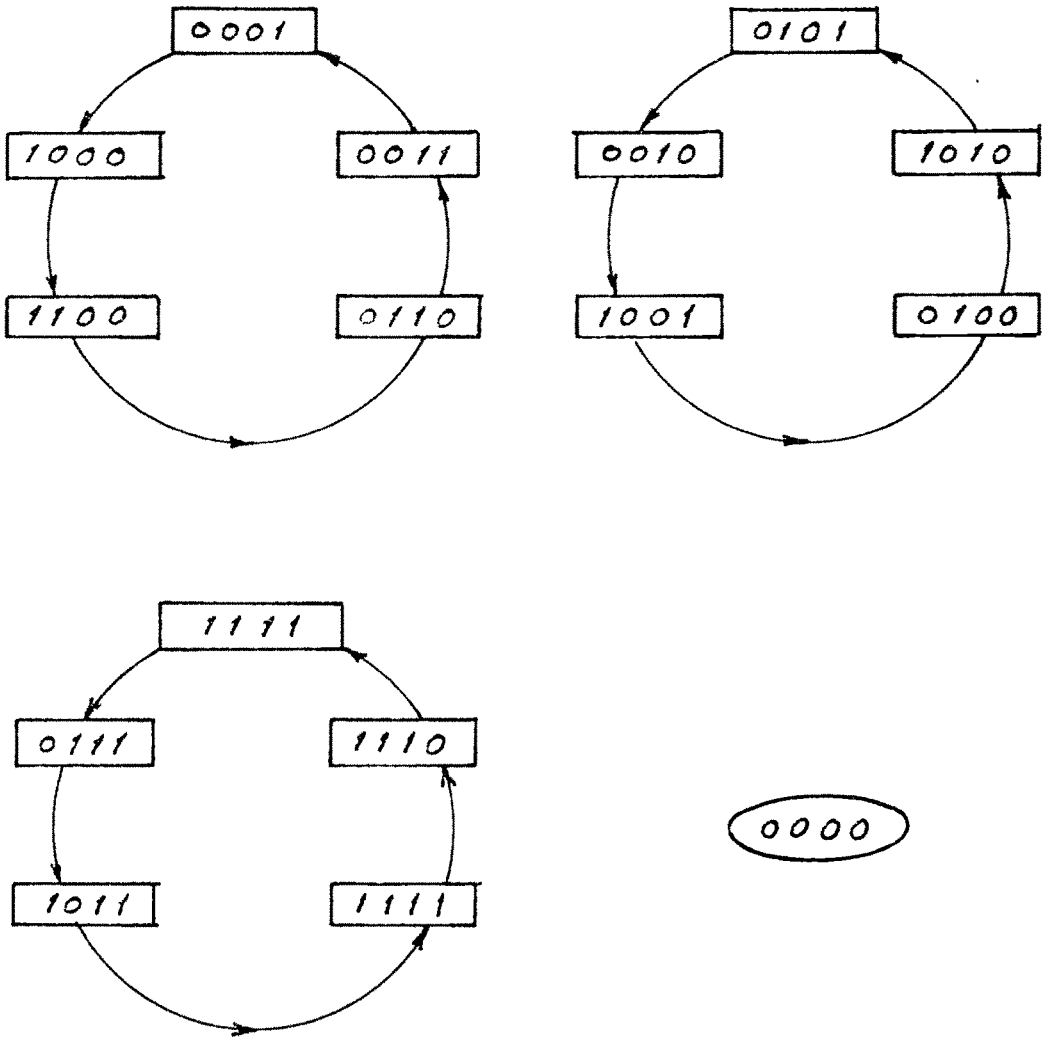


FIG. 1·7 : VECTOR DIAGRAM OF F.S.R. WITH LINEAR RECURRENCE

$$C_r = C_{r-1} \oplus C_{r-2} \oplus C_{r-3} \oplus C_{r-4}$$

$$C_j = C \oplus D^j C , \quad 1 \leq j \leq N$$

are also null sequences of the polynomial.

This means, the modulo-2 sum of any two null sequences of a polynomial is also a null sequence of the polynomial.

20. If F(D) is a factorable delay polynomial of degree n expressed as :

$$F(D) = \prod_{i=1}^{k} F_i(D) ,$$

where the factors $F_i(D)$, i = 1 to k, are all irreducible and primitive (mod-2), then, the complete set of null sequences of F(D) consists of :

(i) The null sequences of its factors, (These are in all k-sequences), and

(ii) all possible sequences that can be obtained by considering the modulo-2 sum of any q(q = 2 to k) of the k sequences of its factors. The period of the resulting sequence equals the L.C.M. of the periods of sequences under consideration.

21. If $F_i(D)$ is any primitive or irreducible delay polynomial, and $G_i(D) = [F_i(D)]^{u_i}$, the period λ_i of the null sequence of $G_i(D)$ is a multiple $e(u_i)$ of the period N_i of $F_i(D)$. That is, $\lambda_i = e(u_i)N_i$, where $e(u_i)$ is given by -

u_i	$e(u_i)$	u_i	$e(u_i)$	
1	1	3-4	4	
2	2	5-8	8	etc.

22. If F(D) is a delay polynomial of the form :

$$F(D) = \prod_{i=1}^{k} G_i(D),$$

and $G_i(D) = [F_i(D)]^{u_i}$, i = 1 to k,

$F_i(D)$ being primitive polynomials (modulo-2), and if,

G_{11} , G_{12} , ... etc. are the null sequences of the term $G_1(D)$,

G_{21} , G_{22} , ... etc. are the null sequences of the term $G_2(D)$,

. . . . .
. . . . . and

G_{k1} , G_{k2}, ... etc. are the null sequences of the term $G_k(D)$,

then, the null sequences of the polynomial F(D) are :

(i) The null sequences of all the terms $G_i(D)$, i = 1, 2, .., k, and

(ii) all possible sequences obtained by modulo-2 sum of the terms $G_i(D)$, i = 1 to k. Here, the sequences that are modulo-2 added should be of different terms $G_i(D)$. The period of the resulting sequence equals the L.C.M. of the different sequences that are modulo-2 added.

23. If F(D) is a delay polynomial of degree m , and is the product of k factors, denoted by $f_i(D)$, i = 1 to k,

all of which are nonrepeated irreducible but nonprimitive modulo-2, then the complete set of null sequences of F(D) are :

(i) The sets of null sequences A_i , i = 1 to k, of period $\frac{2^{m_i} - 1}{M_i}$ of all its factors, where m_i and M_i are degree and period of the factor $f_i(D)$; and

(ii) all possible sequences obtained by modulo-2 sum of the null sequences belonging to the different sets of sequences A_i of its factors.

24. The null sequence of a factorable polynomial could be of period even less than the degree of that polynomial.

25. For a given n, every binary m-sequence is pseudorandom (i.e. pseudonoise) in the sense that it satisfies the following three randomness properties :

(i) The balance property : In each run of the binary m-sequence, the number of ones differ from the number of zeros by 1.

(ii) The run property : Among the runs of ones and zeros in each period, (a pseudorandom sequence is never strictly aperiodic, though the period may be indefinitely long due to deterministic generation device) one half of the runs of each kind are of length 1, one fourth of each kind are of length two, one eighth are of length three, and so on as long as these fractions give meaningful number of runs.

(iii) The correlation property : If a period of the m-sequence is compared, term by term, with any cyclic shift of itself, the number of agreements differ from the number of disagreements by 1.

The auto-correlation function $\phi_{CC}(\tau)$ of an m-sequence C of +1s and -1s of period N digits is defined as :

$$\phi_{CC}(\tau) = \frac{1}{N} \sum_{i=1}^{N} c_i c_{i+\tau}$$

$$= 1 \quad \text{if} \quad \tau = 0$$

$$= -1/N \text{ if } \tau \neq 0$$

where c_r is the rth term in the sequence C and where is the phase shift of the sequence.

$\phi_{CC}(\tau)$ measures the amount of similarity between the sequence and its phase shift. The two-valuedness of the autocorrelation function is of considerable importance in itself.

Example :

Consider the m-sequence C with period N = 31 bits:

C : 1111100110100100001010111011000,..(repeats)

There are 16 1s and 15 zeros, which is adequate to satisfy the randomness property - (i).

Of the 16 runs, half have length one, and one-fourth have length two, one eighth have length three and one-sixteenth have length four. Randomness property -(ii)

The autocorrelation is 1 in phase and -1/31 out of phase. (Randomness property-(iii).

26. If C is an m-sequence of +1s and -1s and C* is the same sequence in which -1s have been replaced by 0s, the crosscorrelation function $\phi_{CC^*}(\tau)$ has the form shown in Fig. 1.8.

Here, $C(t) = \frac{1}{2} C(t) + 1$

so that the cœosscorrelation function $\phi_{CC^*}(\tau)$ is -

$$\phi_{CC^*}(\tau) = \frac{1}{2}\phi_{CC^*}(\tau) + \frac{1}{2T}\int_0^T C(t)\,dt$$

For an m-sequence,

$$\int_0^T C(t)\,dt = t_o \text{ , digit period}$$

since the number of +1s exceeds the number of -1s by one in the period $T = Nt_o$. Thus -

$$\phi_{CC^*}(\tau) = \frac{1}{2}\left[\phi_{CC}(\tau) + \frac{1}{(2^n-1)}\right]$$

Hence, the statement follows from the well-known value of $\phi_{CC}(\tau)$.

27. If an m-sequence of 1s and 0s is added, modulo-2, to the same sequence delayed by rt_o, the resulting sequence is the original sequence C delayed by st_o, where r and s are integers in the range $1 \leq r, s \leq 2^n - 2$, n being the degree of the delay polynomial F(D).

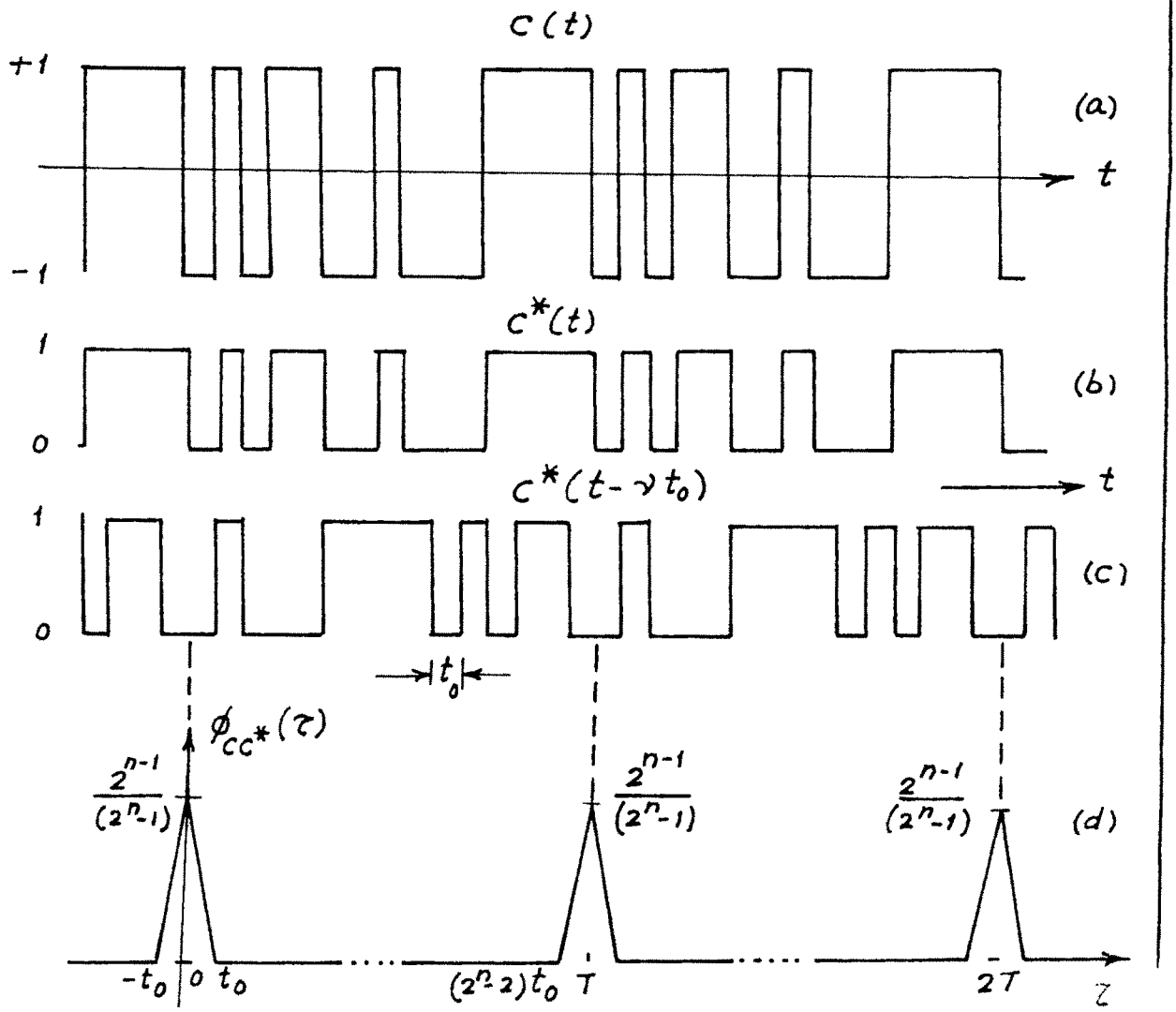


FIG. 1-B (a) LINEAR m-SEQUENCE SIGNAL c(t) OF +1S AND -1S (TIME-VARIATION)

(b) SIGNAL c(t) WITH -1S REPLACED BY ZEROS, DENOTED BY $c^*(t)$

(c) PHASE-SHIFTED VERSION OF THE SIGNAL $c^*(t)$

(d) CROSS-CORRELATION FUNCTION BETWEEN c(t) AND $c^*(t)$

Thus,

$$D^r C \oplus C = (D^r \oplus I)C = D^s C$$

where D is the delay operator which introduces a delay of t_o(digit period), I is the identity operator (i.e. IC = C) and $\oplus$ denotes addition modulo-2.

Example :

Consider m-sequence C generated from a 3-stage fsr with feedback from stages 2 and 3 :

Sequence C : 1110010,...

(delay by t_o) DC : 0111001,...

DC $\oplus$ C=D^5C : 1001011,...

28. If C is any binary sequence of 1s and 0s and C' is defined by the equation -

$$C' = (D \oplus I)C$$

the sequence C' will have a 1 in each position corresponding to the start of a run of 1s or 0s in C, and 0 otherwise.

This property may be verified from the example cited just above.

29. If s_1 is the value of s for r = 1 in the property 27 above, then , for an m-sequence C of a polynomial F(D) of degree n, $(s_1 - 1)t_o$ is equal to the forward time displacement

from the start of the run of (n - 1) zeros to the start of the run of n ones in C, i.e. if C starts with n ones, $D^{S_1-1}C$ starts with (n-1) zeros.

30. Given an n-stage fsr, and (2n - 1) digits of a required maximum-length sequence, it is possible to determine uniquely the feedback connections. (2n - 1) digits are required, since n digits are needed as an initial condition, and (n - 1) additional digits are necessary to specify uniquely which of the stages are to be fedback, besides the nth stage which is always fedback.

31. Every m-sequence exhibits the following structural property:

When an m-sequence C of period N is multiplied by any of its phase shifted versions, there occur exactly

$$L_1(\tau) = \frac{N+1}{4} \text{ number of } (1-1) \text{ pairs},$$

$$L_0(\tau) = \frac{N-3}{4} \text{ number of } (0-0) \text{ pairs},$$

and $$L(\tau) = \frac{N+1}{2} \text{ number of } (0-1) \text{ and } (1-0) \text{ pairs.}$$

Evidently, $L_1(\tau)$, $L_0(\tau)$, $L(\tau)$ are independent of the phase shift τ. Hence, invariance of $L_1(\tau)$ and $L_0(\tau)$ for any nonzero τ may be said to be the necessary and

sufficient condition for a sequence to be of maximum length (i.e. for it to be called a pseudorandom sequence)

32. An m-sequence (pseudorandom binary sequence) possesses a perfect analogy to a cyclic difference set .

A difference set (Hall 1956) is defined as a set of k integers with the following property -

If the differences between all possible combinations of two of the k numbers are formed, followed by modulo-e, then all integers between 1 and e - 1 occur exactly λ times. Integers e, k and λ are called the parameters of the difference set.

According to the structural feature of the m-sequence stated under property 31 above, there are exactly L_1 digit pairs in state 1 (and digits apart) within one period, for any $\tau \neq 0$. Translated to the number set, this means that there are exactly $L_1(i, j)$ pairs for which :

$$(d_i - d_j) (\text{mod. } N) = \tau \quad , \qquad \tau \neq 0 \ (\text{mod } N)$$

where d_i, $d_j (i \neq j)$ are the members or elements of the m-sequence.

33. Changing the signal levels (signal being the continuous version of the sequence) associated with the two states in an m-sequence signal to any values, the result is

again an m-sequence signal. Proof of this property follows from property 31, whereby $L_1(\tau)$, and $L_0(\tau)$ have no reference to the signal-levels.

From this it also follows that the complement of an m-sequence is also an m-sequence.

34. Sampling an m-sequence by a sampling period of r digits, where r is relatively prime to the period of the sequence, leads to an m-sequence. This is because the autocorrelation for τ of the resulting sequence is identical to the auto-correlation for $r\tau$ of the original sequence.

From this, it follows that the time inverse of an m-sequence is also an m-sequence.

35. If it is known that a periodic binary sequence is a maximum length sequence for some polynomial, then it is easy to examine the sequence and determine the polynomial itself.

Example :

Consider the sequence with a period of 15 digits given below :

111100010011010,...

In it, there are certain to be four places where all but one of the four successive digits are zero. The digits immediately following each of these groups are the coefficients a_1 , a_2 , a_3 and a_4 in the polynomial given by -

$$I \oplus a_1 D \oplus a_2 D^2 \oplus a_3 D^3 \oplus a_4 D^4$$

From the examination of the above sequence it follows that the required polynomial is :

$$(I \oplus D^3 \oplus D^4)$$

36. A duality between polynomials and their null sequences can be found by dividing I by the polynomial in question.

Example :

Dividing the 3rd degree polynomial $I \oplus D \oplus D^3$ into I -

$$\frac{I}{I \oplus D \oplus D^3} = I \oplus D \oplus D^2 \oplus D^4 \oplus D^7 \oplus D^8 \oplus D^9 \oplus D^{11} \oplus D^{14} \oplus ..$$

$$= (I \oplus D \oplus D^2 \oplus D^4)(I \oplus D^7 \oplus D^{14} \oplus D^{21} \oplus ...)$$

$$= (I \oplus D \oplus D^2 \oplus D^4) \; / \; (I \oplus D^7)$$

Therefore,

$$(I \oplus D \oplus D^3)(I \oplus D \oplus D^2 \oplus D^4) = I \oplus D^7$$

The exponents of the terms $I \oplus D \oplus D^2 \oplus D^4$ can be related to the 1s in the null sequence for $I \oplus D \oplus D^3$ which has initial state... 001 ; as shown below :

$$\cdots\cdots \; 00(\underset{\downarrow}{1} \quad \underset{\downarrow}{1} \quad \underset{\downarrow}{1} \quad 0 \quad \underset{\downarrow}{1} \quad 0 \quad 0)\underset{\downarrow}{1}11$$

$$D^0 \oplus D^1 \oplus D^2 \oplus D^4 \qquad (D^7)$$

37. Any polynomial which has an even number of terms (regardless of its degree) has a factor $I \oplus D$.

38. The square of a polynomial of the form :

$$I \oplus D \oplus D^2 \oplus \ldots \oplus D^n$$

is

$$I \oplus D^2 \oplus D^4 \oplus \ldots \oplus D^{2n} .$$

This property can be utilized in the calculation pertaining to the delayed version of m-sequences. For instance, given that -

$(I \oplus D^1 \oplus D^6)C = 0$, it is required to find the feedback connections for $D^{30}C$.

Continually squarring (modulo-2) the given eqn. we get -

$$I \oplus D^2 \oplus D^{12} = 0$$

$$I \oplus D^4 \oplus D^{24} = 0$$

Now, $D^{30}C = D^6 . D^{24}C = D^6(D^4 \oplus I)C$

$= (D^{10} \oplus D^6)C = (D^4 . D^6 \oplus D^6)C$

$= D^4C(D^1 \oplus D^0) \oplus C(D^1 \oplus D^6)$

$= (D^6 \oplus D^5 \oplus D^4)C$

39. Among the delay polynomials over modulo-2,

$$[F(x)]^{2^t} = F(x^{2^t})$$

Let $t = 1$, and $F(x) = (I \oplus D)x$

$$(I \oplus D)^2 x = (I \oplus D \oplus D \oplus D^2)x = (I \oplus D^2)x$$

For the case that $t > 1$, and $F(x)$ consists of more than two terms, the property can be proved by finite induction on the number of terms. Then, for the general case, the property follows from finite induction on t.

40. The polynomial $(D \oplus D^{2^k})$ can be written as the product of all irreducible polynomials, the degrees of which divide k - all once.

For instance,

$$(D \oplus D^{2^4}) = D(I \oplus D)(I \oplus D \oplus D^2)(I \oplus D \oplus D^4)$$
$$(I \oplus D^3 \oplus D^4)(I \oplus D \oplus D^2 \oplus D^3 \oplus D^4)$$

The proof of this theorem is given by W.W. Peterson.

41. If a polynomial $F(D)$ divides $I \oplus D^s$, then $F(D)$ divides $I \oplus D^{sq}$ for $q = 0, 1, 2, \ldots$.

$I \oplus D^0 = 0$, for $q = 0$, the theorem is trivial. If $q = 1, 2, \ldots$

$$I \oplus D^{sq} = (I \oplus D^s)(I \oplus \ldots \oplus D^{(q-2)s} \oplus D^{(q-1)s})$$

42. If F(D) divides $I \oplus D^s$, then F(D) has a period t which divides s.

43. It is possible to find the delay polynomial which generates a large number of null sequences with a specified cycle length as shown below :

Suppose that it is desired to find the delay polynomial that generates a large number of sequences with cycle length 21 digits.

It follows from Table (1.6) that there are two nonprimitive irreducible polynomials of degree 6 with period 21:

$$F_1(D) = I \oplus D \oplus D^2 \oplus D^4 \oplus D^6 ,$$

and $$F_2(D) = I \oplus D^2 \oplus D^4 \oplus D^5 \oplus D^6$$

Hence, both polynomials yield the following sequences :

1 cycle of length 1 bit (all-zero sequence)

3 cycles of length 21 bits.

This may be represented as :

1(1), 3(21)

Then $F_1(D) \cdot F_2(D)$

leads to the following number of sequences :

1(1), (3 + 3 + 9.21)(21)

To give twice the number of sequences, the characteristic polynomial $F_1(D) \cdot F_2(D)$ can be multiplied by $I \oplus D$. The resulting polynomial is as follows :

$$F(D) = F_1(D) \cdot F_2(D) \cdot (I \oplus D)$$
$$= I \oplus D^2 \oplus D^3 \oplus D^5 \oplus D^6 \oplus D^7 \oplus D^8 \oplus D^{10} \oplus D^{11} \oplus D^{13}.$$

which yields the following number of sequences :

2(1) , 390(21)

which is in accordance with the fact that -

$$2.1 + 390.21 = 2^{13}.$$

44. If $C = \{c_r\}$ is an m-sequence, then c_{qr} equals C except for a phase shift, when $q = 1, 2, 4, 8, \ldots 2^{n-1}$.

The numbers $1, 2, 4, 8, \ldots 2^{n-1}$ are called multipliers of the sequence, and they are collectively known as the multiplier group.

Example :

Let $C = \{c_r\}$: 1110100 , ...

$q = 2$, $\{c_{2r}\}$: 1110100 , ...

$q = 4$, $\{c_{4r}\}$: 1110100 , ...

while,

$q = 3$, $\{c_{3r}\}$: 1001011 , ...

$q = 5$, $\{c_{5r}\}$: 1001011 , ...

45. Given the irreducible polynomial -

$$F(D) = \sum_{i=0}^{n} a_i D^i ,$$

Let $F_1(D) = \sum_{i=0}^{n} a_i D^{n-i}$. Then $F_1(D)$ is also irreducible. The shift register sequence corresponding to $F_1(D)$ is simply the time inverse of the sequence corresponding to F(D). Thus, if F(D) is a maximal polynomial, so does $F_1(D)$.

46. If F(D) is an irreducible polynomial, so is $H(D) = F(I \oplus D)$, since any factorization of H(D) would factor F(D). However, H(D) may fail to have maximum exponent, even though F(D) has.

Example :

If $F(D) = I \oplus D^3 \oplus D^4$ with its null sequence of period N = 15 digits, then,

$$H(D) = I \oplus (I \oplus D)^2 \oplus (I \oplus D)^4$$

$$= I \oplus D \oplus D^2 \oplus D^3 \oplus D^4$$ has null sequences of period 5 digits.

47. Given an irreducible polynomial of degree n, it is possible to get as many as five others by means of properties (45) and (46).

48. If $F(D) = \sum_{i=0}^{n} a_i D^i$ is a maximal polynomial of degree n, then,

$$F_1(D) = \sum_{i=0}^{n} a_i D^{2^n-1}$$

is an irreducible polynomial, but not necessarily a maximal one.

However, if 2^q-1 is prime, where $q = 2^n-1$, then F(D) must be a maximal polynomial.

Example :

$F(D) = I \oplus D \oplus D^2$ is a maximal polynomial

$F_1(D) = I \oplus D \oplus D^3$ is also maximal polynomial.

But applying the same transformation to $F_1(D)$, we obtain -

$F_2(D) = I \oplus D \oplus D^7$ which is not a maximal polynomial.

Applying the transformation again to $F_2(D)$, we get -

$F_3(D) = I \oplus D \oplus D^{127}$ which is a maximal polynomial.

49. If $\{c_r\}$ is an m-sequence of period N, and if q_o , q_1 ,...q_ℓ is any set of representatives of the proper cyclotomic cosets' S_1 , S_2 , ... , S_ℓ , then

$\{c_{rq_o}\}$, $\{c_{rq_1}\}$, ... , $\{c_{rq_\ell}\}$ are all m-sequences of period N.

Concept of coset : (Golomb 1964)

The integers n (degree of the polynomial F(D)) corresponding to sequence c_r) from 1 to N - 1 with no factors in common with N form a multiplicative Abelian group with

respect to operation : multiplication modulo-2. The numbers 1, 2, 4, ... 2^{n-1} form a 'sub-group' with n elements. This sub-group, when multiplied by any other element of the group, yields a coset.

For example : If $N = 2^5 - 1 = 31$, the multiplicative group consists of integers 1 to 30. The decomposition into cosets is :

S_o	: 1	2	4	8	16
S_1	: 3	6	12	24	17
S_2	: 9	18	5	10	20
S_3	: 27	23	15	30	29
S_4	: 19	7	14	28	25
S_5	: 26	21	11	22	13

50. If $\{c_r\}$ is an m-sequence with period N, then $\{c_{qr}\}$ is again an m-sequence, with the same period if $(q , N) = 1$. If both $(q_1 , N) = 1$ and $(q_2 , N) = 1$, then $\{c_{q_1 r}\} = \{c_{q_2 r}\}$ (except for the starting point) if and only if q_1 and q_2 belong to the same cyclotomic coset modulo-N.

51. Every m-sequence $\{c_r\}$ of period N has a phase shift $\{e_r\}$ such that the value of e_r depends only on the cyclotomic coset to which r belongs modulo-N and not on the exact value of r.

Example : The sequence 1110100 with period N = 7, is left termwise invariant by the multiplier group (1, 2, 5), but is inverted by the multiplier group (3, 6, 5). It is seen that :

$$e_o = 1$$
$$e_1 = e_2 = e_4 = 1$$
$$e_3 = e_5 = e_6 = 0$$

52. The number of distinct values assumed by the cross-correlation $\phi_{12}(\tau)$ of two m-sequences C_1 and C_2, each of period N, can never exceed Y(N), the number of cyclotomic coset modulo-N.

Example :

$N = 7,$

C_1 : 1110100, ...

C_2 : 1001011, ...

$\phi_{12}(0) = 1, \phi_{12}(1) = \phi_{12}(2) = \phi_{12}(4) = 2$

$\phi_{12}(3) = \phi_{12}(6) = \phi_{12}(5) = 3.$

53. The power spectrum of an m-sequence is a line spectrum and has an envelope of (sin x / x), reaching the first value of zero at the frequency of the clock pulse.

This may be verified by using the fact that the power density spectrum $\phi_x(t)$ of a function x(t) is simply the Fourier transform of the autocorrelation function of x(t). Thus the power density spectrum of an m-sequence signal C(t) is of the form -

$$\phi_C(t) = \sum_r \frac{a^2 t_o (N + 1)}{N} \left[\frac{\sin r\pi / N}{r\pi / N} \right]^2$$

where a is the amplitude of the signal C(t) corresponding to the m-sequence C, t_o is the digit period, and

$$\frac{\sin r\pi / N}{r\pi / N} = 1 \quad .. \quad (\text{approx. for } r << N)$$

Therefore, the power spectrum has an amplitude of the order of $(N + 1)a^2 t_o / N$ for low frequencies, and this falls by 3 dB at a frequency given by

$$\frac{\sin r\pi / N}{r\pi / N} = 0.7071$$

or $r = N / 3$ (approximately)

The effective frequency band covered by a maximum length is, therefore, from -

$$f = 1 / Nt_o \text{ to } 1 / 3t_o \quad (\text{Hz})$$

The harmonic seperation of the spectrum is $1 / Nt_o$, and the spectrum amplitude at zero frequency is dt approximately $a^2 t_o (N + 1) / 2N$.

54. Every m-sequence of period N can be written as a fourier expansion : The Fourier coefficients b_k are given by :

$$b_k = \frac{1}{N} \sum_{i=1}^{N} b_i e^{2\pi ki / N}$$

Let an m-sequence $\{c_r\}$ be phased so that $\{c_{2r}\} = \{c_r\}$. Then, $b_{k_1} = b_{k_2}$ whenever k_1 and k_2 belong to the same coset modulo-N.

55. Every m-sequence is perfect.

If $C = \{c_r\}$ is any binary sequence with period v, and if the autocorrelation $\phi_{CC}(\tau)$ of $\{c_r\}$ satisfies

$$\phi_{CC}(\tau) = \sum_{i=1}^{v} c_i c_{i+2}$$

$$= \alpha \quad \text{if } \tau = 0 \text{ (modulo-v)}$$

$$= \beta \quad \text{if } \tau \neq 0 \text{ (modulo-v)}$$

then, $\{c_r\}$ is called a perfect sequence.

In view of this definition and property (25), the statement is true.

1.9 GENERATION OF MAXIMAL AND NONMAXIMAL LINEAR BINARY SEQUENCES AND STUDY OF THEIR STATISTICAL CHARACTERISTICS

The theory of generation of cyclic binary sequences by means of linear feedback shift register is already discussed in section (1.2). To study their statistical characteristics and to verify some of their properties, the generation of the linear binary maximal as well as nonmaximal sequences is experimented. Experience is briefly described in this section in the generation and measurement of autocorrelation function of the m-sequence signal (commonly known by the name pseudorandom binary signal, abbreviated as prbs).

The feedback shift register (fsr) is composed of two kinds of elements : (1) Unit-delay elements, and (2) modulo-2 adders. Master-Slave J.K. Flip-Flop with integrated circuits is used as the unit delay element, and the modulo-2 adder (i.e. the not-equivalent logic circuit) consists of two 'AND' and one 'NOR' logic gates. These circuit elements (integrated circuits) are supplied by ' Instruments and systems, New Delhi.' In this binary network (i.e. the binary feedback shift register sequence generator) the states 1 and 0 correspond to the analogue-levels 5 volts and 0 volts respectively.

1.9.1 Working of the master J.K. flipflop with integrated circuits

The block diagram and symbolic representation of the master-slave J-K flipflop with integrated circuits are shown in Fig. 1.9. Here (J , K) are the inputs and (C ,$\bar{C}$) are the corresponding outputs. T is the clock input and R is the reset, which is normally left on '0'. Flipping it to 1 and back to zero sets the flipflop in C = 0 condition (i.e. $\bar{C}$ = 1).

The operation of a J - K flipflop can be divided in 2 Reset-Set clocked flipflops. Gates 1, 2 with steering gates 3, 4 form a slave flipflop. The gates 5, 6 with the steering gates 7, 8 form the master flipflop. In addition, the outputs C and $\bar{C}$ are coupled back in gates 7 and 8.

Let us examine what happens when J = 1, K = 1 and C = 1 (i.e. the flipflop is in state 1). When the clock pulse arrives, the voltage at first rises from 0 to 1 for a short time. The gate 8 then has all its inputs 1 giving rise to 0 output. Gate 7 has J = 1, $\bar{C}$ = 0 and clock = 1, hence its output is 1. This activates the gate 6, putting the master flipflop in 0 condition (i.e. A = 0, B = 1).

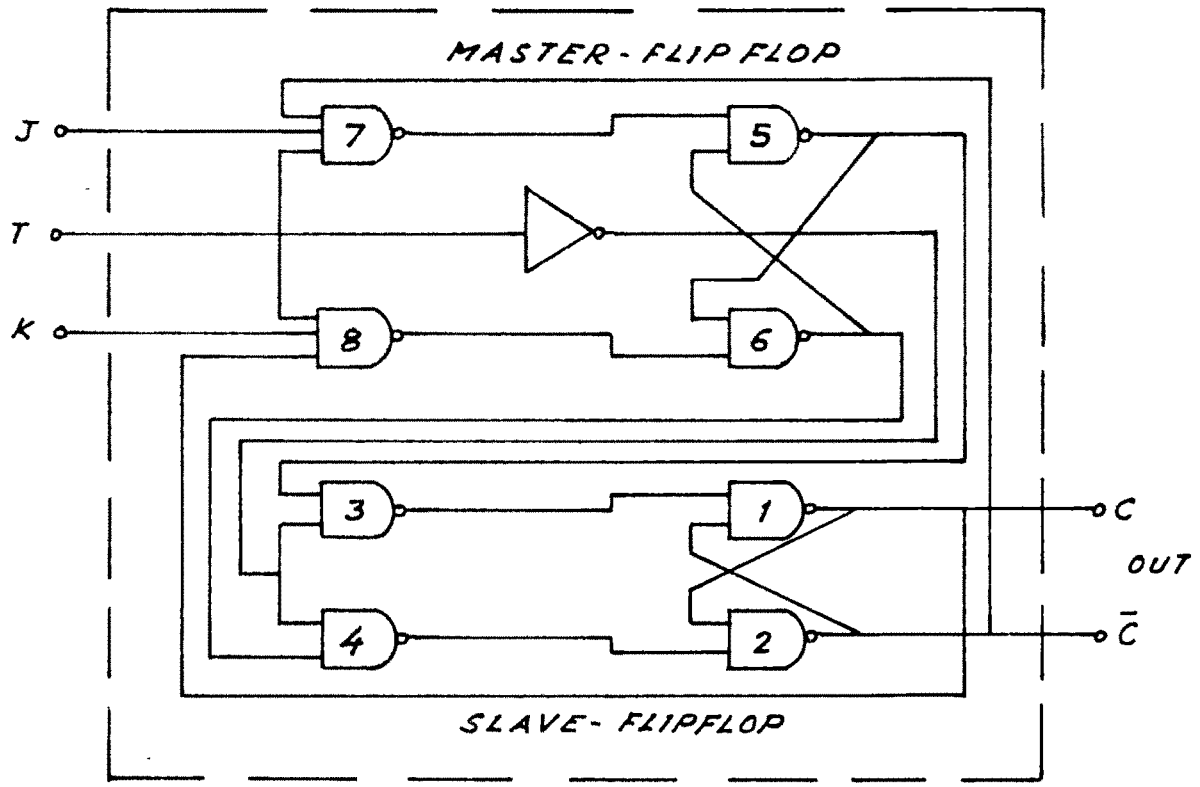


FIG. (a)

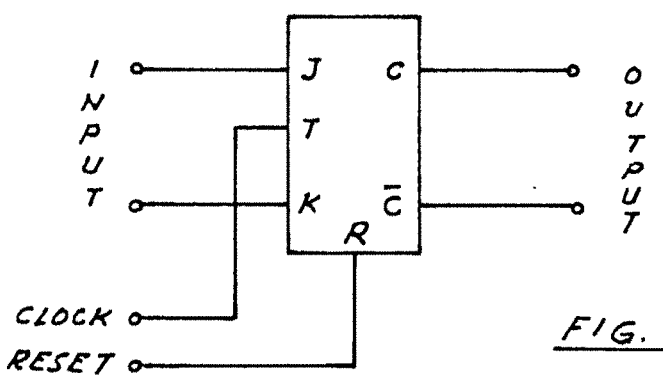


FIG. (b)

NAND

FIG. 1·9 : (a) SYMBOLIC REPRESENTATION OF MASTER J·K. FLIP-FLOP.

(b) BLOCK DIAGRAM OF THE FLIP-FLOP

The clock pulse is now returning to 0 from 1, and through the inverter provides a 1 clock signal to gates 3 , 4. The slave flipflop with B = 1 is reset to give 0 output (C = 0, and $\overline{C}$ = 1).

The total outcome is that the flipflop has inverted its state and also the input conditions at gates 7 and 8 are inverted (through C and $\overline{C}$). The next clock pulse will throw the flipflop in 1 condition, like a toggle switch.

The output condition for all the input conditions (Truth Table) of the Master J-K flipflop is shown in the following table.

Table 1.12. Truth Table for J-K Flipflop

Initial outputs		Inputs		Final outputs	
C	$\overline{C}$	J	K	C	$\overline{C}$
1	0	1	1	0	1
1	0	0	0	1	0
1	0	1	0	1	0
1	0	0	1	0	1
0	1	1	1	1	0
0	1	0	0	0	1
0	1	1	0	1	0
0	1	0	1	0	1

1.9.2 Modulo-2 adder

The modulo-2 adder is nothing but a not-equivalent logic circuit. A block diagram of this logic circuit, consisting of 2 'AND' gates and a 'NOR' gate is shown in Fig. 1.10. The truth table of the 2 AND-NOR Gate combination is given in Table 1.13 below. The symbol ' $\oplus$ ' in all the figures of the linear binary feedback shift register circuit shown in this chapter represents this circuit.

Table 1.13. Truth Table for modulo-2 adder of Fig. 1.10

A	$\overline{B}$	$\overline{A}$	B	Output
1	0	0	1	0
1	1	0	0	1
0	0	1	1	1
0	1	1	0	0

1.9.3 J-K feedback shift register generating an m-sequence

The linear binary feedback shift register is depicted in Fig.1.11. As shown, the outputs '$\overline{C}$s' from the second and fifth stages are fedback to the first stage through the modulo-2 adder. Hence, the characteristic equation of the shift register may be written as -

$$F(D)\ C = (I \oplus D^2 \oplus D^5)C = 0$$

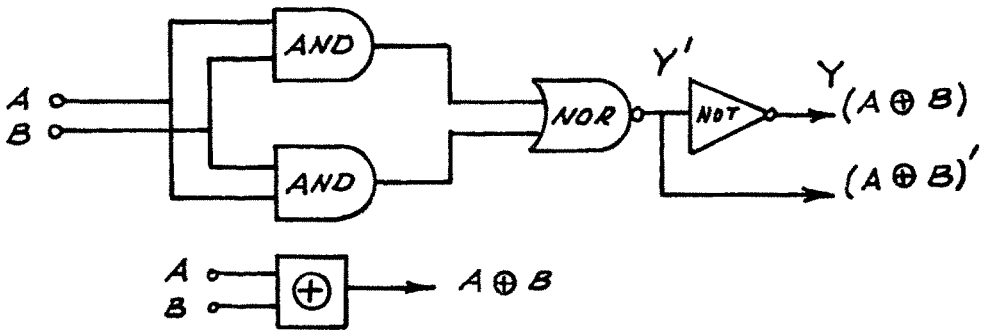


FIG. 1·10 REALIZATION OF MODULO-2 ADDITION

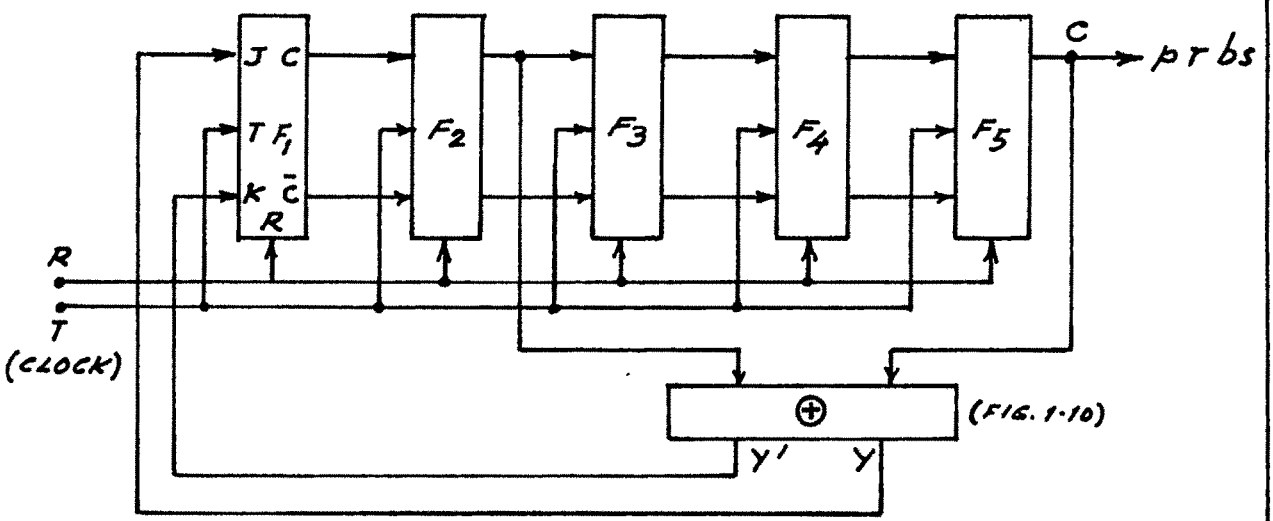


FIG. 1·11 PRACTICAL REALIZATION OF PRBS USING MASTER J.K. FLIP-FLOPS

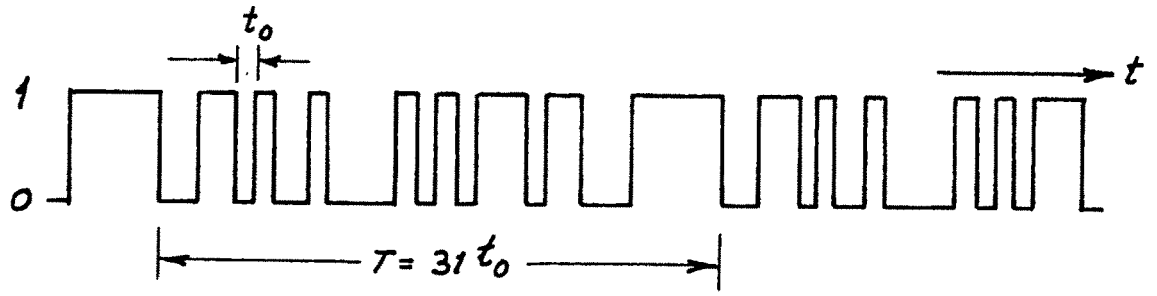


FIG. 1·12 OUTPUT OF THE 5-STAGE PRBS GENERATOR

where C is the cyclic binary sequence representing the output of the modulo-2 adder (i.e. the input sequence to the first stage of the fsr).

At first all the flipflops viz. D_1 , D_2 , D_3 , D_4 and D_5 are reset, thereby C - outputs are in 0 - state and $\overline{C}$ - outputs in 1 - state. On completion of the resetting, the K - input of the 1st flipflop is in 0 state.

A clock signal of period t_o = 0.5 msec is then applied. At the first clock pulse, D_1 goes to $\overline{C}$ = 0, but D_2, D_3, D_4 and D_5 remain in $\overline{C}$ = 1 as their K inputs are 1. Now the information at the K-input of D_1 is made 0 again. At the second pulse, therefore, flipflops D_1 and D_2 go to $\overline{C}$ = 0 whereas D_3, D_4 and D_5 still remain in $\overline{C}$ = 1. Finally, on the occurance of 31st clock pulse, the initial setting (all $\overline{C}$ = 1) is restored. As the clock signal continues the same cycle is repeated again and again. The content of the fsr at any instant of time is called its state, and may be considered as a binary number. The succession of states in the above 5 - stage fsr is as shown below :

As seen from the succession of states, all the $2^5 - 1$ nonzero states are described before the output at any stage starts repeating. As the clock pulse is continuous , the output is the continuous version of the m-sequence. Thus, an

Table 1.12. $F(D)\ C = (I \oplus D^2 \oplus D^5)C = 0$

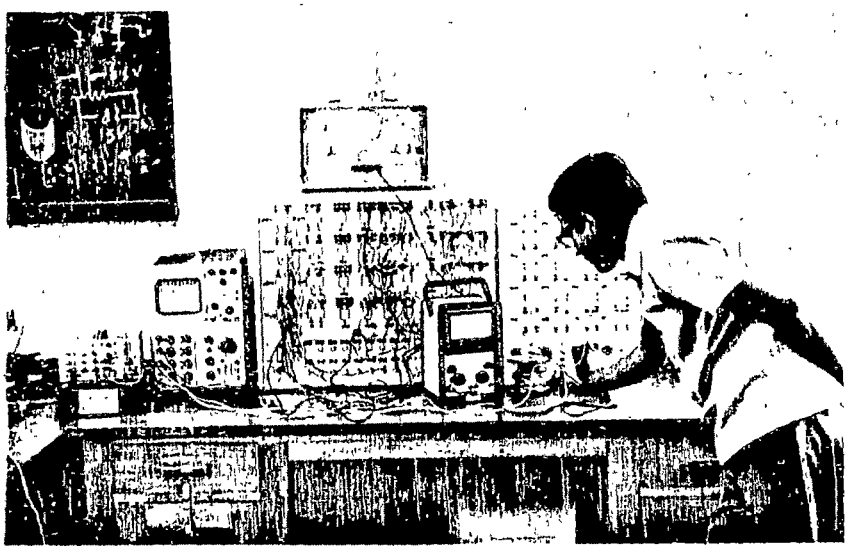
State No.	Stage number of fsr				
	1	2	3	4	5
0	1	1	1	1	1
1	0	1	1	1	1
2	0	0	1	1	1
3	1	0	0	1	1
4	1	1	0	0	1
5	0	1	1	0	0
6	1	0	1	1	0
7	0	1	0	1	1
8	0	0	1	0	1
9	1	0	0	1	0
10	0	1	0	0	1
11	0	0	1	0	0
12	0	0	0	1	0
13	0	0	0	0	1
14	1	0	0	0	0
15	0	1	0	0	0
16	1	0	1	0	0
17	0	1	0	1	0
18	1	0	1	0	1
19	1	1	0	1	0
20	1	1	1	0	1
21	0	1	1	1	0
22	1	0	1	1	1
23	1	1	0	1	1
24	0	1	1	0	1
25	0	0	1	1	0
26	0	0	0	1	1
27	1	0	0	0	1
28	1	1	0	0	0
29	1	1	1	0	0
30	1	1	1	1	0
31	1	1	1	1	1

m-sequence signal or pseudorandom binary signal is generated using the master J-K feedback shift register. Fig. 1.12 shows the so generated prbs.

1.9.4. Generation of nonmaximal sequences

The cycle structures of all the possible nonmaximal polynomials of order 5 are observed by setting the possible initial conditions in the 5-stage feedback shift register. The distinct cycles associated with the different polynomials are stated below. The polynomials generating sequences that are reverse of each other are grouped here. As may be seen, the polynomials $I \oplus D^5$, $I \oplus D \oplus D^4 \oplus D^5$, $I \oplus D^2 \oplus D^3 \oplus D^5$ and $I \oplus D \oplus D^2 \oplus D^3 \oplus D^4 \oplus D^5$ have self-reverse property.

Delay Polynomial	Associated Cycle Set
$I \oplus D^5$	:(10100),(11110),(11100),(11000),(10000),(10101),(1)
$I \oplus D \oplus D^5$	:(11111010100110001000),(1110010),(110).
$I \oplus D^4 \oplus D^5$	:(11111000010001100 1010),(1110100),(110).
$I \oplus D \oplus D^2 \oplus D^5$	:(11110010000110),(1100010),(1110100),(10),(1).
$I \oplus D^3 \oplus D^4 \oplus D^5$	:(11110110000100),(1101000),(1110010),(10),(1).
$I \oplus D \oplus D^3 \oplus D^5$	:(1111000100110 10),(000011101100101),(1).
$I \oplus D^2 \oplus D^4 \oplus D^5$	:(111101011001000),(000010100110111),(1).
$I \oplus D \oplus D^4 \oplus D^5$	:(11110000),(11010010),(1110),(1100),(1000),(10),(1)
$I \oplus D^2 \oplus D^3 \oplus D^5$	:(111101000010),(111000),(1100),(110),(100),(10),(1)
$I \oplus D \oplus D^2 \oplus D^3 \oplus D^4 \oplus D^5$	:(111100),(110000),(101000),(111010),(110),(100)(1



Experimental Set Up

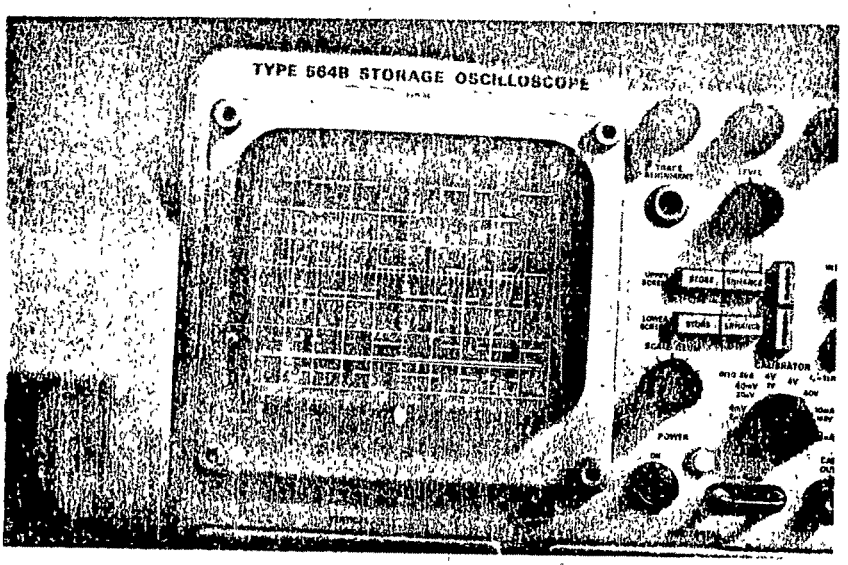


Fig.1.12 (B) : (a) 31-bit prbs generated by the maximal polynomial $I \oplus D^2 \oplus D^5$

(b) Binary multiplicator output of Fig.1.18

(c) Output of symmetry circuit of Fig. 1.18

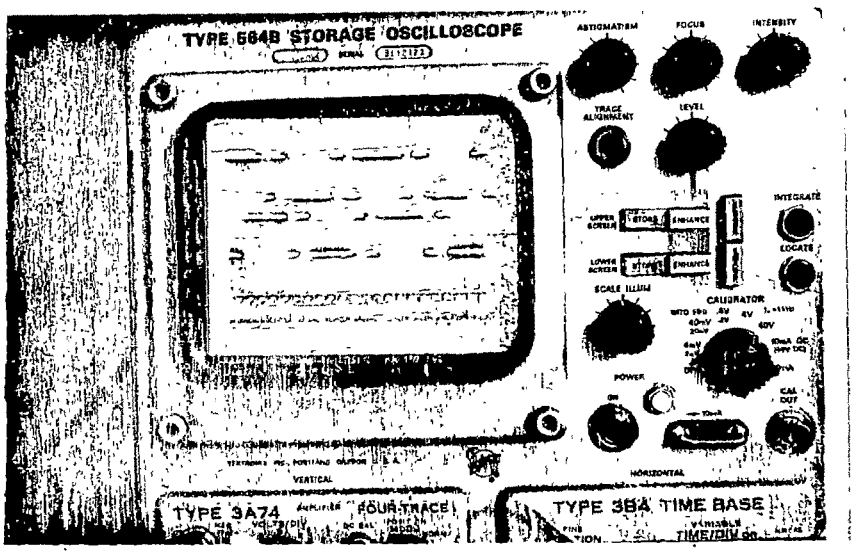


Fig.1.12(C):12-bit nonmaximal sequence and its phase shifted version generated by the factorable polynomial $I \oplus D^2 \oplus D^3 \oplus D^5$

1.9.5 Measurement of autocorrelation function of prbs

Theoretical considerations -

The autocorrelation function of a continuous signal x(t) is defined as -

$$\phi_{xx}(\tau) = \lim_{T \to \infty} \frac{1}{2T} \int_{-T}^{T} x(t).x(t-\tau)\,dt \quad \ldots\ldots \quad (1.29)$$

Since the m-sequence signal (pseudorandom binary signal) is periodic, its autocorrelation is written as -

$$\phi_{xx}(\tau) = \frac{1}{Nt_o} \int_{o}^{Nt_o} x(t)\ x(t-\tau)\,dt \quad \ldots\ldots \quad (1.30)$$

As an example, consider the m-sequence signal x(t) shown in Fig. (1.13) generated by a 3-stage fsr whereby the outputs of 2nd and 3rd stages are fedback to the 1st stage through linear logic. The autocorrelation function of the signal, by definition, is :

$$\phi_{xx}(\tau) = \frac{1}{7t_o} \int_{o}^{7t_o} x(t)\ .\ x(t-\tau)\,dt$$

When the phase shift τ lies in the region $0 \leq \tau \leq t_o$, the product $x(t).x(t-\tau)$ is shown in Fig. 1.13 and the autocorrelation function is -

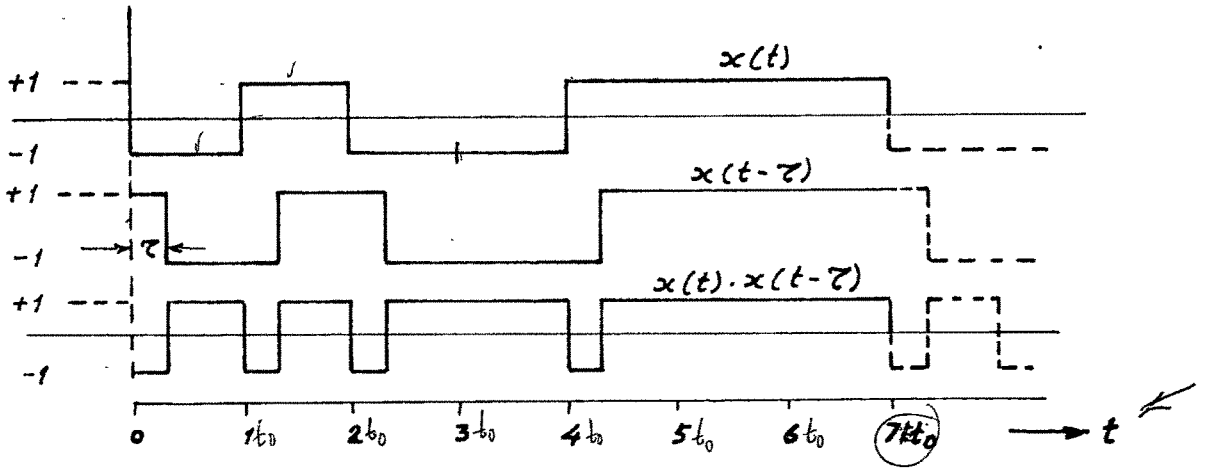


FIG. 1·13 PRODUCT SIGNAL $x(t)\cdot x(t-\tau)$ FOR $0 \leq \tau \leq t_0$

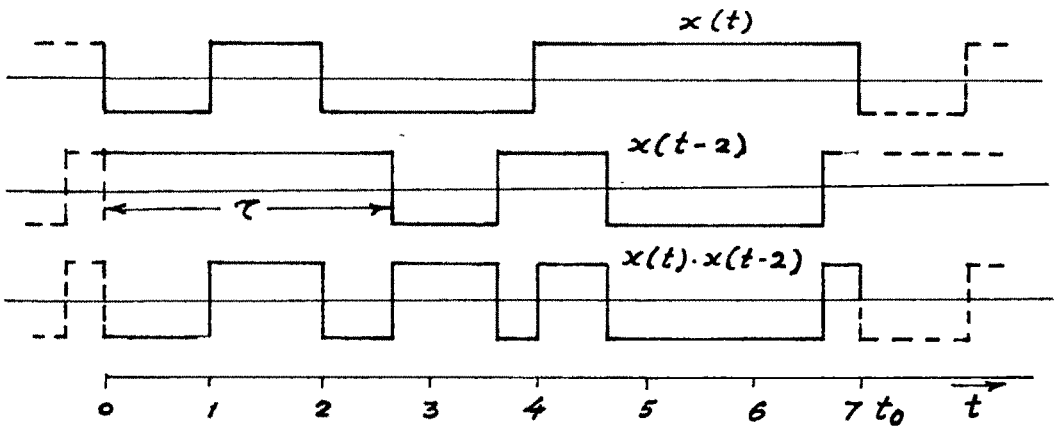


FIG. 1·14 PRODUCT SIGNAL $x(t)\cdot x(t-\tau)$ FOR $2t_0 \leq \tau \leq 3t_0$

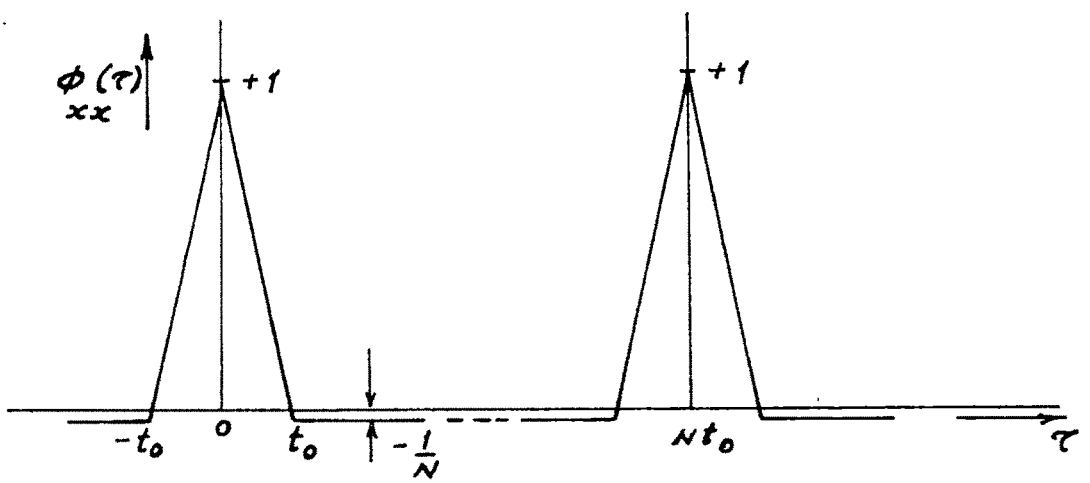


FIG. 1·15 AUTO CORRELATION FUNCTION OF A P.R.B.S

$$\phi_{xx}(\tau) = \frac{1}{7t_o}\int_{o}^{7t_o} x(t).x(t-\tau)\,dt$$

$$= \frac{1}{7t_o}\Big[\int_{o}^{\tau} dt + \int_{\tau}^{t_o} dt - \int_{t_o}^{t_o+\tau} dt$$

$$+ \int_{t_o+\tau}^{2t_o} dt - \int_{2t_o}^{2t_o} dt + \int_{2t_o+\tau}^{4t_o} dt - \int_{4t_o}^{4t_o+\tau} dt$$

$$+ \int_{4t_o+\tau}^{7t_o} dt\Big] = 1 - \frac{8}{7}\frac{\tau}{t_o}$$

When the phase shift τ lies in the region $t_o \leq \tau \leq 6t_o$, the product $x(t).\ x(t-\tau)$ for $2t_o \leq \tau \leq 3t_o$ is shown in Fig. 1.14. The autocorrelation function of x(t) in this case is :

$$\phi_{xx}(\tau) = \frac{1}{7t_o}\int_{o}^{7t_o} x(t)\ .\ x(t-\tau)\,dt$$

$$= \frac{1}{7t_o}\Big[-\int_{o}^{t_o} dt + \int_{t_o}^{2t_o} dt - \int_{2t_o}^{\tau} dt + \int_{\tau}^{\tau+t_o} dt$$

$$- \int_{\tau+t_o}^{4t_o} dt + \int_{4t_o}^{\tau+2t_o} dt - \int_{\tau+2t_o}^{\tau+4t_o} dt$$

$$+ \int_{\tau+4t_o}^{7t_o} dt\Big] = \frac{-1}{7}\ .$$

The above results indicate that the autocorrelation function of an m-sequence signal x(t) of period Nt_o is :

$$\phi_{xx}(\tau) = 1 - \frac{N+1}{N}\left|\frac{\tau}{t_o}\right|, \qquad |\tau| \leq t_o$$

$$= -\frac{1}{N}, \qquad t_o \leq |\tau| \leq (N-1)t_o$$

Apparently the autocorrelation function $\phi_{xx}(\tau)$ of the pseudorandom binary signal is periodic with period Nt_o, where $N = 2^n-1$, n being the degree of the fsr generating the signal x(t). Fig. (1.15) shows the autocorrelation function of the prbs.

As N is made larger, the autocorrelation function considered overone cycle becomes more like that of white noise - i.e. an impulse function at the origin. It is this property which makes the prbs so useful.

Practical considerations -

The theoretical results derived above are verified by carrying out the measurement of the autocorrelation function of the 31 digits length m-sequence signal, the generation of which is described in section 1.9.3.

The circuit for the purpose must be in accordance with the eqn. (1.30) -

$$\phi_{xx}(\tau) = \frac{1}{Nt_o}\int_0^{Nt_o} x(t)\cdot x(t-\tau)\,dt.$$

Clearly, the measurement of $\phi_{xx}(\tau)$ involves the following operations -

(i) Shifting the signal x(t) by the required time τ to obtain $x(t - \tau)$,

(ii) Multiplication of x(t) with $x(t - \tau)$,

(iii) Averaging the product $x(t).x(t - \tau)$ over the period of x(t).

Generation of delayed replicas of x(t) -

If x(t) is defined as the basic m-sequence signal obtained from the logical output of the shift register (activated by the master clock of period t_o), then, the delayed versions of x(t), viz. $x(t - t_o)$ to $x(t - nt_o)$ are readily available from the register. The remaining delayed versions, $x[t - (n + 1)t_o]$ to $x[t - (N - 1)t_o]$ are realized by the addition of (N - n) binary stages to the existing generator.

This straight forward approach is attractive in that all the stages are synchronized with the shift-line clock pulses and the delays are progressive along the shift register stages.

If, however, only a small number of selected copies are needed, this method is wasteful of equipment, because the number of extra stages required is determined by the largest relative delay among the copies, rather than the number of copies sought. For this purpose several methods have been proposed

In section (2.5) of the following chapter, these are briefly discussed and a quick method of evaluating the feedback connections for any required delay is broughtforth.

For the determination of $\phi_{xx}(\tau)$ in the region $0 \leq |\tau| \leq t_o$ we need to shift the signal x(t) in this range of τ. For this purpose, a clock signal of period $t_s = \frac{1}{q} t_o$, (q=1, 2, 4, 8..) is derived using flipflops as shown in Fig. (1.18).

Multiplication of x(t) with x(t - τ) -

Since the signals x(t) and x(t - τ) are both binary, their product can be obtained with the help of the binary logic elements as under -

Let us compare the product operation in the field (-1, 1) with the modulo-2 addition operation in the field (0, 1).

•	-1	1
-1	1	-1
1	-1	1

⊕	0	1
0	0	1
1	1	0

It is seen that there is equivalence between multiplication and negated modulo-2 addition : i.e.

•		⊕
+1	≡	1
-1		0

Utilizing this equivalence, the binary multiplicator is assembled from 2 'AND' and 1 'NOR' gates as shown in Fig.1.16.

It is already stated that within the binary network composed of the integrated logic elements, any wire is capable of being, at any instant of time, in either 1-state or in 0-state. The 1-state corresponds to an analogue level of 5 volts, and the 0-state to a level of 0-volts. Hence, the putput of the multiplicator is simply an unsymmetrical binary signal. It is, therefore, necessary to pass the multiplicator output through a symmetrical network, before proceeding to average the product signal $x(t).x(t-\tau)$. In Fig. (1.18), the block denoted by the symbol 'S' after the multiplicator is this symmetry-circuit, the output of which is maintained at $\pm$ 2.5 volts. As a result, a proportionality factor (k) enters into the measured value of the autocorrelation function (Fig. 1.18).

Averaging the signal $k\ x(t)\ .\ x(t-\tau)$

The average value of the product signal $kx(t).x(t-\tau)$ is arrived at with the help of a first order low pass filter. The time constant of the filter is kept much larger than the shift pulse period so as to obtain accurate values of the autocorrelati function. The justification of this follows from the steps written below -

TRUTH-TABLE

A	B	C
0	0	1
0	1	0
1	0	0
1	1	1

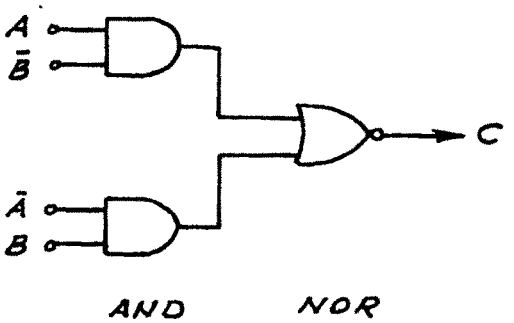


FIG. 1·16 BINARY MULTIPLICATION

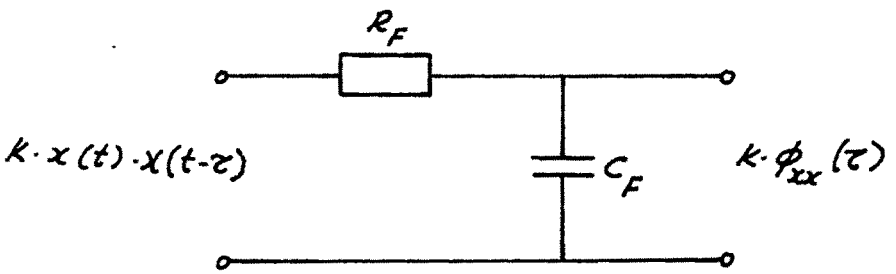


FIG. 1·17 AVERAGING WITH A LOW-PASS FILTER

For the output of the low-pass filter shown in Fig.(1.17), we may write -

$$\Psi(t, \tau) = k \int_{-\infty}^{+\infty} g_F(t-u).\{x(u).x(u-\tau)\}\,du \quad \ldots \quad (1.32)$$

where $g_F(t)$ is the impulse response of the filter.

For the first order filter shown in the figure, the impulse response is -

$$g_F(t) = \frac{V}{T_F} e^{t/T_F} \quad \ldots \quad \ldots \quad \ldots \quad (1.33)$$

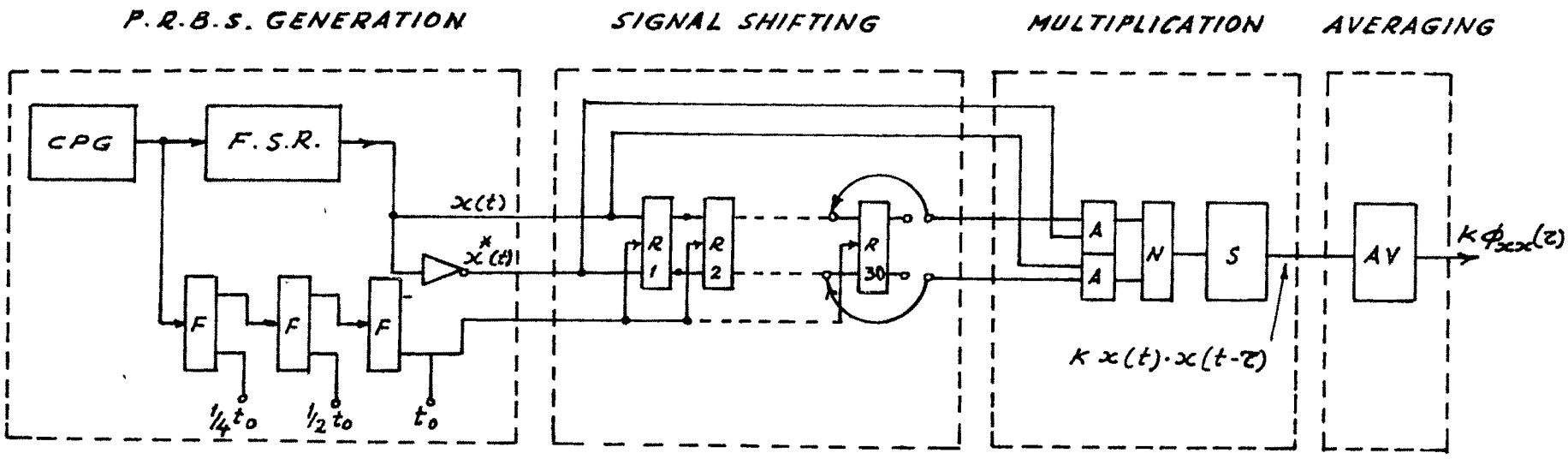
where T_F is its time-constant.

For V = 1,

$$\Psi(t, \tau) = \frac{k}{T_F} \int_{-\infty}^{+\infty} e^{\frac{-t-u}{T_F}} . x(u-\tau).x(u)\,du \quad \ldots \quad (1.34)$$

$$\simeq k\,\phi_{xx}(\tau) \quad , \text{ for } T_F \gg t_o \quad \ldots \quad (1.35)$$

Fig. (1.18) depicts the block diagram of the circuit used for the measurement of the autocorrelation function of 31-bit length prbs. A vacuum tube volt meter is used to obtain the values of $k\,\phi_{xx}(\tau)$. The measured autocorrelation function with (i) $0 \leq |\tau| \leq t_o$ and (ii) $t_o \leq |\tau| \leq N t_o$ is shown in Fig. (1.19) and (1.20). (t_o is the shift pulse period)



CPG: CLOCK PULSE GENERATOR

FSR: FEED BACK SHIFT REGISTER

F: FLIP-FLOP

R: SHIFT REGISTER

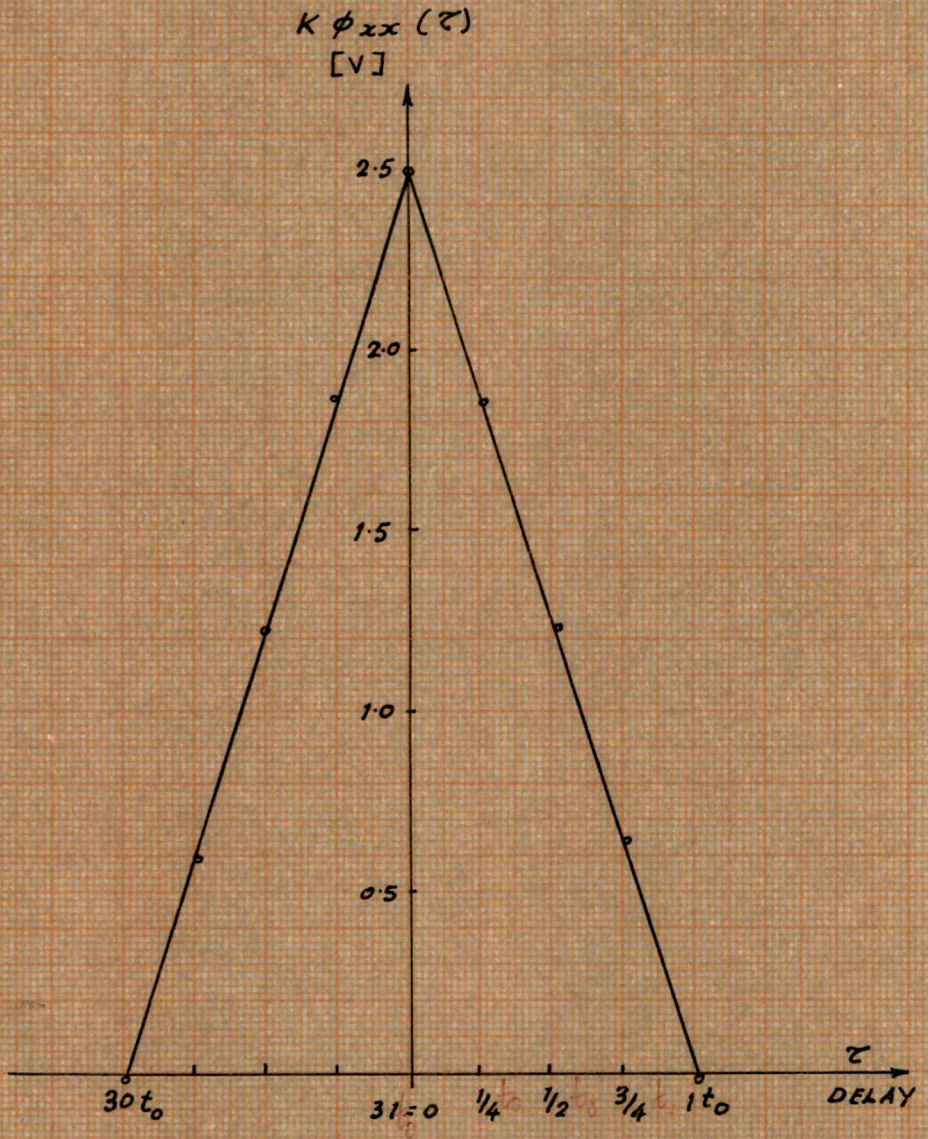
A: AND GATE

N: NOR GATE

S: SYMMETRY CIRCUIT

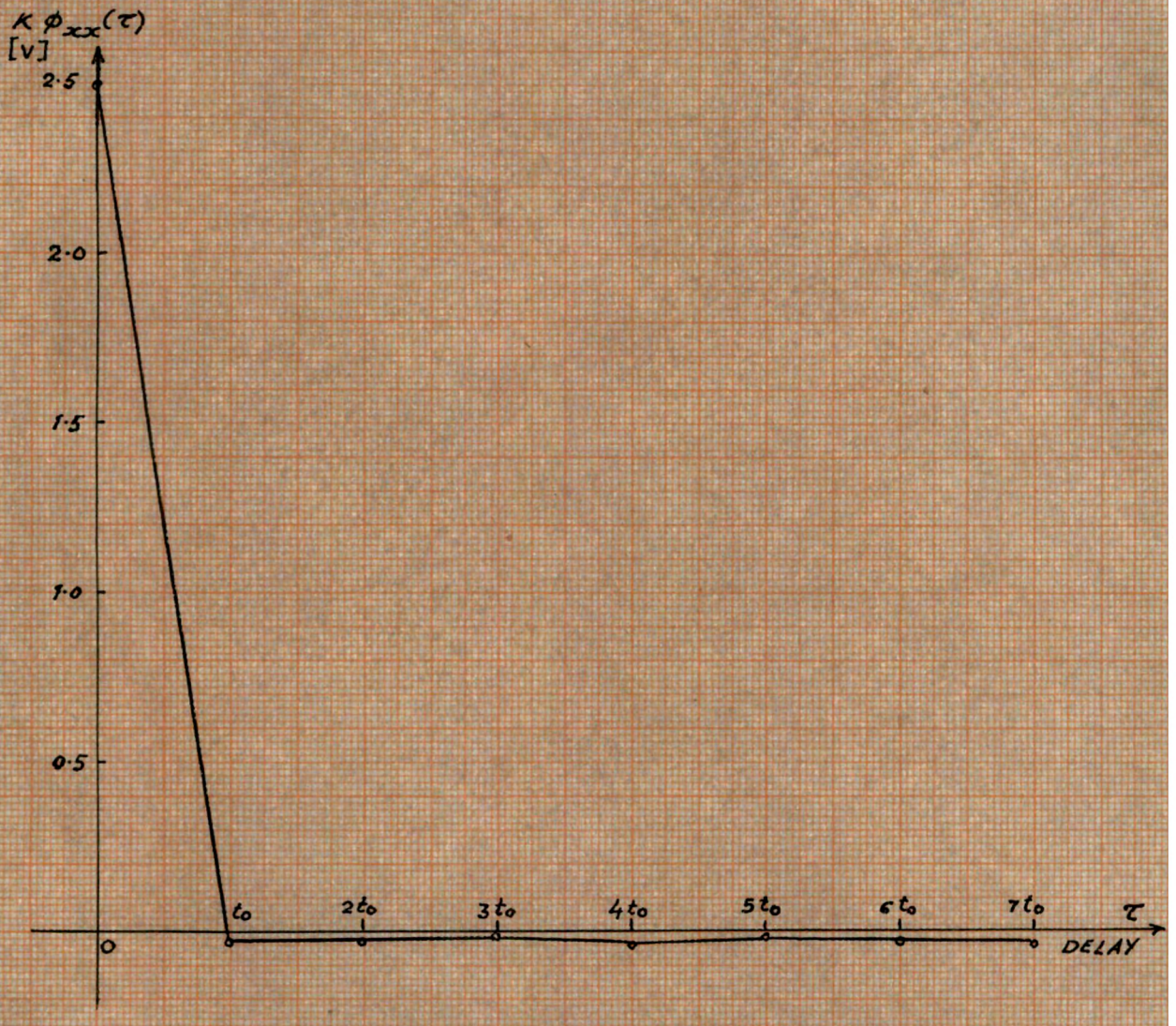
AV: AVERAGING DEVICE

FIG. 1·18 MEASUREMENT OF $\frac{\phi_{xx}(\tau)}{\tau}$



REGION OF SHIFT, τ: $0 \leq |\tau| \leq t_0$

FIG. 1·19 MEASURED AUTOCORRELATION FUNCTION OF THE 31 - BIT PRBS



REGION OF SHIFT, τ: $0 \leq \tau \leq N t_0$

FIG. 1·20 MEASURED AUTOCORRELATION FUNCTION OF THE 31-BIT PRBS

As seen from the measured autocorrelation function (Fig. 1.19 and 20), in the region $0 \leq \tau \leq t_p$ the measured values are in agreement with the theoretical values. But, in the region $t_p \leq \tau \leq (N-1)t_p$, the measured values slightly differ from the theoretical ones. The fluctuations in the power supply and the presence of noise voltages are primarily responsible for such deviations.

1.10 PRINCIPAL AREAS OF APPLICATION AND ADVANTAGES OF BINARY SHIFT REGISTER SEQUENCES

The theory of shift register sequences has found major applications in a wide variety of technological situations. It is the purpose of this section to list the principal areas of applications and briefly to state the major advantages of using the sequences.

1.10.1 Areas of application

1. Secure and limited access code generators

Encipherment : A shift register sequence may be added, modulo-2 to a message written in binary digits so as to act as a 'key' to the message. The decipherment consists of adding the key (modulo-2) to the coded message.

Multiple address coding : Different portions of a long shift register sequence can be made use of by assigning

characteristic addresses to a large number of individuals, aircraft, and so forth. For example, such a system assigning ten-bit segments of a sequence of length 1023 to each of 64 outlying weather stations, was installed to monitor rainfall information in the vicinity of Calcutta.

2. Efficiency code generators

Error detection and correction : The nomral method of error detection and correction for messages of binary digits is to add extra digits which are related in special ways to the message digits. In a chain code the digits in the chain which follow any particular pattern are generated in precisely this way, and so chain codes can be applied directly to error detection and correction.

Range radar applications : For range radar applications in environments where excessive background noise is present, a CW signal using an m-sequence, has the property that its autocorrelation function can be recovered in spite of the excessive noise present.

3. Counting and frequency division

There are several counting applications, both in computing and general electronics, where the use of the

binary number sequence yields no special advantage. In such cases considerable advantage may be given by using the chain code together with suitable diode coincidence detectors. The chain code counter completes the count operation in the shift time of one element. It realizes, with economy of components, the maximum counting speed of the transistor circuits used.

Another general electronic application is the frequency division of variable-frequency input pulses. Here again, an n-stage chain code generator giving a ratio of less than (2^n-1) can be employed.

4. Mathematical models

Random bit generator : In spite of the fact that a feedback shift register is a deterministic device, it can be used as a model for the outcome of a coin-tossing experiment. In fact, mathematicians suggested the use of shift registers for the generation of random numbers for Monte Carlo statistical techniques.

Finite state machines : The feedback shift register can be taken as a simple example of an autonomous finite state machine.

Markov processes : The de Bruijn diagram for sequential behaviour of an n-stage fsr is also the Markov state diagram for a binary channel with statistical dependence limited to

n bits into the past. Although the shift register usage represents only a limiting case of the Markov process (with transition probabilities 1 and 0), the topological characteristics discovered by shift register research is interpretable in terms of the general Markov process.

5. System identification by cross-correlation

It is well-known that the dynamic response of a linear system can be obtained by using white noise as the input and cross-correlating it with the output of the system. However, white noise (characterised by a flat power spectrum of infinite bandwidth) is a mathematical fiction : it is awkward to generate a flat power spectrum at the low frequencies and difficult to achieve repeatable results. Another drawback results from the need to perform cross-correlation over a long period of time.

So much so, use of binary random noise as test signal in correlation analysis has been considered. But, here too, difficulties have been experienced in processing as well as controlling the parameters of the test signal and the results of the system dynamics obtained were not very satisfactory.

More recently use has been made of the m-sequence signals as test perturbations as they exhibit properties in correlation similar to those of white noise, even though they are generated from a deterministic device. An advantage of these cyclical test signals over random signals is that, since the properties are deterministic, unequivocal expressions for the system dynamics can be obtained in a noise free system. Further, in the usual case where noise is present in the system, the degree of uncertainty in the results is contributed solely by the system noise, and there is no uncertainty due to the test signal.

1.10.2 Advantages of binary shift register sequences

The following are the main factors that are primarily responsible for the increasing interest in the shift register sequences in the various technological situations.

1. The generation and processing of the shift register sequence is remarkably simple.
2. The maximum length shift register sequences has an orthogonality constraint between the various time shift of the sequence, which leads to linearly independent parity checks, and also to perfect two-level autocorrelation.
3. The properties of shift register sequences will not drift or deviate in any way with time, temperature or other environmental changes.

4. The power of the m-sequence generated by the fsr can be made to lie in the interested band of frequencies, and is not a fixed parameter. Further, the amplitude and total power of the m-sequence may be controlled precisely by choosing the parameters of the sequence.

5. Every periodic binary sequence can be generated using feedback shift register. Furthermore, given the logical configuration of an fsr, the sequence can be described or given a sequence, the corresponding structure of the fsr can be determined.

6. For counting and frequency division, a shift register is a simpler and more natural device than the normal binary counter.

7. Linear shift register sequences exhibit certain randomness properties that are adequate for most applications of Monte Carlo techniques.

8. Many important properties of shift register sequences (e.g., cycles that are branchless or information-loss less lead to the study of more general autonomous finite state machines.

9. Since the periodic shift register m-sequence is well defined, any experiment using one can be repeated with exactly the same input.

10. The cyclic shift register m-sequence, although deterministic, exhibit properties in correlation similar to those of white noise. This property has been made use of in system identification by correlation methods, with no uncertainty in the results due to the m-sequence test signal.

1.11 SUMMARY

The sequential behaviour of linear binary feedback shift register has been analyzed in some detail in this chapter. The results of the study, as reported here, are encouraging in that. A strong relation is established between the feedback shift register logical structure on the one hand, and the network sequential behaviour on the other. Useful properties of the feedback shift register and its properties are discussed. The practical generation of the sequences and verification of some of their properties was successfully experimented. Mention is also made of the principle areas of application and advantages of the sequences.

In the ~~next~~ following chapter, the use of binary m-sequences as test perturbations in system identification by correlation method ~~will~~ is ~~be~~ discussed and a new correlation scheme for the purpose ~~will~~ is be presented. Furthermore, a simple and quick method of evaluating the binary shift register connections for providing any desired delayed version of the generated m-sequence (needed in the above correlatioh experiment) ~~will be~~ is brought-forth.
