C H A P T E R III

LINEAR MULTILEVEL SHIFT REGISTER SEQUENCES

		Page
3.1	Introduction	228
3.2	Working of autonomous linear multilevel feedback shift register	231
3.3	Delay elements and modulo-p logic	235
3.4	Analysis of sequential behaviour of linear multilevel shift registers	236
3.5	Determination of the delay polynomial from its null sequence	249
3.6	Some properties of p-nary delay polynomials and their null sequences	261
3.7	Generation of delayed replicas of linear p-level maximum length sequences	273
3.8	A structural property of a p-nary m-sequence	296
3.9	Generation of pseudorandom signals corresponding to m-sequences over GF($p=2^2$)	304
3.10	Summary	314

LINEAR MULTILEVEL SHIFT REGISTER SEQUENCES

3.1 INTRODUCTION

The correlation method of dynamic analysis of a single input / single output linear system using two - level shift register m-sequence (pseudorandom binary sequence) as test perturbations has been discussed in the previous chapter. In practice, most systems or in general non-linear and multi-variable. However, because of several advantages associated with the crosscorrelation technique, a search for suitable test signals for implementing the crosscorrelation principle to the identification of nonlinear and multivariable systems has been necessitated. In this connection, the multilevel pseudorandom sequences have been found to be superior to the orthodox 'two-state' m-sequences in some respects, and their practical realization has also been shown to be quite feasible. (Zierler 1959, Elspas 1959, Gyftopoulos and Hooper 1964, Briggs and Godfrey 1966, Simpson 1966, Godfrey 1966, Gardiner 1966, Clarke and Godfrey 1967, Hooper and Gyftopoulos 1967, Selway and Bell 1968, Chang 1968, Rydin and Hooper 1969, Ream 1970, Kerlin 1971, Barker 1970,72).

For instance the investigation by Godfrey (1966) proves that the use of 3-level m-sequences reduces the number of cross-correlation experiment required to determine the impulse response of the linear channel of a system with an amplitude nonlinearity. The recent works of the researchers as mentioned in the above references further emphasise the usefulness of multilevel pseudorandom sequences. Early contributions in this area by Zierler (1959), Elspas (1959), and Hartmanis (1959) deal, respectively, with the mathematical formulations of multilevel (i.e. p-level) sequences, their generations using linear circuitry and use in sequential coding networks.

In view of their superiority over the binary sequences, this chapter is devoted to the development of the theory of multilevel linear shift register sequences and to the practical generation of these sequences by means of binary logic elements. Specifically the content of this chapter is as follows :

In Section 3.2 the working of an autonomous linear multi-level feedback shift register is explained and the meaning and classification of the p-nary characteristic delay polynomials of the above shift register and the sequence it produces, are stated. Section 3.3 gives a brief account of the elements that comprise the autonomous multilevel network. Section 3.4 advances the ideas concerning (i) generating function and

(ii) C_k-transform, which are introduced in Chapter 1, to the present p-nary situation and describes procedures for evaluating null sequences that are associated with all the groups of delay polynomials, classified in Section 3.2. Section 3.5 considers the problem of determining the delay polynomial that corresponds to a given p-nary null sequence. Section 3.6 states some of the useful properties of p-nary shift registers and their sequences. In Section 3.7, a number of methods for finding the p-level shift register connections for providing delayed versions of the basic m-sequence are described. Here, firstly, the presently available techniques for the delay generation for the binary case are extended to the general p-nary case. Secondly, a new method of finding a shift register connections for the delayed version is described that is based on the concept of generating function associated with the p-nary sequence under consideration. In Section 3.8 a structural property of p-nary m-sequence is broughtforth, which helps to determine as to whether a given p-level linear shift register sequence is pseudorandom or otherwise In Section 3.9, an attempt is made to describe the generation of pseudorandom signals, based on m-sequences corresponding to GF($p = 2^m$, m an integer), by means of binary logic elements, which is successfully experimented.

The analysis upto Section 3.8 is limited to multilevel linear shift registers, which remain stable in 'p' states, p being a prime integer.

3.2 WORKING OF AUTONOMOUS LINEAR MULTILEVEL FEEDBACK SHIFT REGISTER

Consider a general autonomous network shown in Fig.(3.1), where no input is present except a clock-pulse of period t_o. Each of the rectangles labelled, D_1, D_2, ..., D_n is a multistable delay-element or shift register which delays the variable on which it operates by a time period equal to t_o. If t_o is chosen as the standard to express the amount of time delay, each delay element or shift register causes a delay of one unit. Thus a delay of r units, D^r, may be obtained by connecting r identical elements in series as shown in the figure. The number of stable states of each shift register is assumed to be the same and equals a fixed prime value 'p' which remains 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 delay elements. In the absence of the feedback-path (Fig. 3.1), the series string of p-nary shift registers gets emptied by the end of nth clock-pulse. However, outputs of some of the n-registers may be fedback into the first register through a feedback logic device to keep the autonomous network active. That is, leads from some of the n-delay elements feed into a logic device

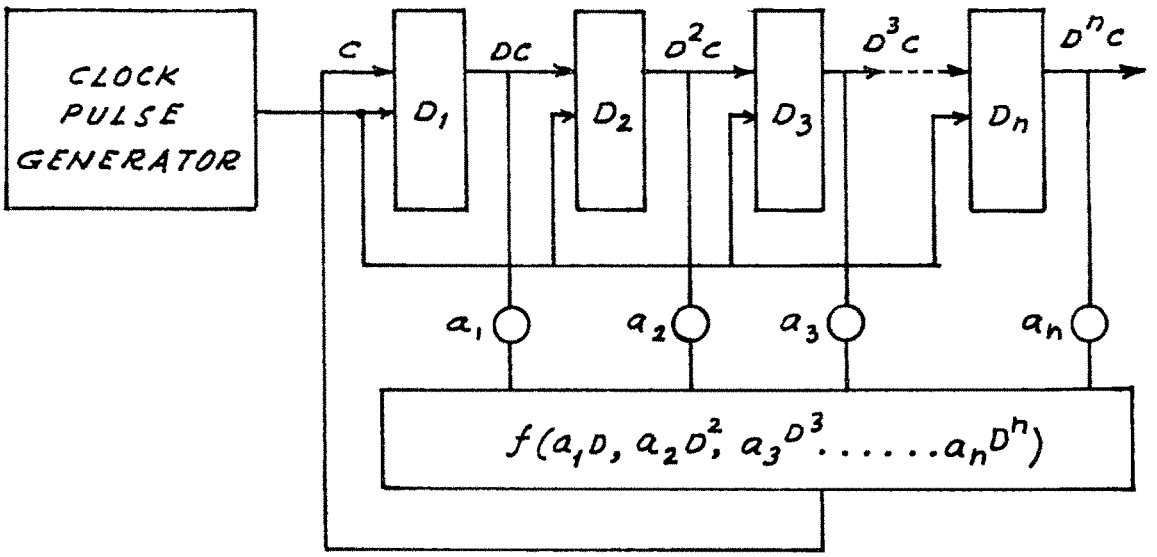
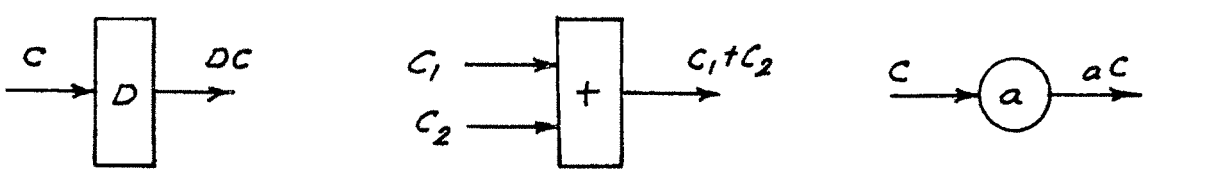


FIG. 3·1 GENERAL DIAGRAM OF AN AUTONOMOUS SYSTEM WITH MULTI STABLE DEVICE



(a) UNIT-DELAY (b) MOD-P ADDER (c) MOD-P MULTIPLIER

FIG. 3·2 LINEAR-LOGIC AND DELAY ELEMENTS.

which provides input to the first delay-element. These delay elements are called the stages of the multilevel feedback shift register. If n-stages are employed, the feedback shift register (fsr) is then 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 p-nary number. Evidently, the maximum number of distinct possible states of such a feedback shift register is p^n. On the application of a train of clock-pulses, the network undergoes, from its initial state, a cyclic succession of states, the number of which depends on the feedback logic and initial state. Thus a p-nary sequence of certain periods may be realized at the output of each stage.

If $C = (c_o, c_1, c_2 \ldots)$ represents the p-nary periodic output sequence of the feedback logic device shown in Fig.(3.1) the autonomous multilevel shift register may be described by the equation :

$$f(a_1DC, a_2D^2C, \ldots a_nD^nC) = C \quad \ldots \quad \ldots \quad (3.1)$$

The eqn. (3.1) is thus seen to characterize the sequential behaviour of the p-nary shift register and is accordingly called as its ' characteristic equation '. However, if the feedback logic may be expressed in the form :

$$f(a_1DC, a_2D^2C, \ldots, a_nD^nC) = (a_1D + a_2D^2 + \ldots + a_nD^n)\, C$$

where the coefficients 'a_i' may assume any of the p values in

the modular field of integers (0, 1, 2, ..., p-1), and where the symbol '+' denotes the 'modulo-p addition' ; the autonomous network shown in Fig. (3.1) is called 'linear'. Thus for a linear system, the characteristic equation takes the form :

$$C = (a_1 D + a_2 D^2 + \ldots + a_n D^n)\, C \quad \text{(Mod.-p addition)} \qquad \ldots (3.2)$$

In accordance with modulo-p arithmetic, stated in the Section 3.3, the characteristic equation of the multilevel feedback shift register may also be expressed as :

$$[(p-1) + a_1 D + a_2 D^2 + \ldots + a_n D^n]\, C = 0 \quad \ldots (3.3)$$

This appears in the closed form :

$$\left[+ \sum_{i=0}^{n} a_i D^i\right] C = 0 \qquad \ldots \qquad \ldots \qquad \ldots \qquad (3.3a)$$

where $a_o = (p-1)$.

The expression within the brackets in eqn. (3.3), which is composed of characteristic delays acting on the p-nary variable C is called ' Delay-Polynomial' of the linear p-nary shift register, and may be represented as F(D) :

$$F(D) = (p-1) + a_1 D + a_2 D^2 + \ldots + a_n D^n \quad \ldots (3.4)$$

The delay polynomials that describe the sequential behaviour of the linear multilevel shift registers may be classified based on their factorable features as :

A : Primitive delay polynomials,

B : Irreducible but non-primitive delay polynomials,

C : Factorable delay polynomials.

Referring back to the multilevel shift register of Fig. (3.1), under the linearized conditions, any signal flowing through the network is capable of being, at each instant of time, in any one of the p-stable states represented by the digits 0, 1, 2, ..., p-1. Since modulo-2 logic is used in the feedback path, the state represented by 'n zeros' becomes a trivial one. Thus the maximum number of the distinct possible states now becomes $p^n - 1$, where n is the degree of the feedback shift register. Furthermore, the presence of identical unit-delays (p-stable shift registers) signifies that the change over of one stage to another is instantaneous. The operations performed by the system on the signals flowing through it constitute linear operations of delay, mod-p addition, and mod-p multiplication by a constant scale factor over the modular field of integers 0, 1, 2, ..., p - 1. A brief account of these three kinds of operations will now be given before proceeding to the analysis of the multilevel feedback shift registers and their sequences.

3.3 DELAY-ELEMENTS AND MODULO-P LOGIC

The autonomous network discussed here is composed of arbitrary interconnections of three kinds of elements, namely, (a) Unit delay elements, (b) Modulo-p adders, and (c) Modulo-p multipliers. The symbols used for these elements are shown in Fig. (3.2a,b,c).

As each delay element or shift register causes a delay of one digit period, the term ' D^iC ' means that the variable C is delayed by i digits by allowing it to flow successively through I delay elements. The digit period is determined by the frequency of the master-clock, which activates the feedback shift register.

The modulo-p addition and modulo-p multiplication correspond to the usual arithmetic addition and multiplication followed by the removal of all multiples of p. The table below illustrates this aspect.

Table 3.1 :

mod-p addition

p = 3,+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

mod-p multiplication

p = 3, .	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

p = 5,+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

p = 5, .	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

3.4 ANALYSIS OF SEQUENTIAL BEHAVIOUR OF LINEAR MULTILEVEL SHIFT REGISTERS

This section describes two methods to derive analytically the sequential behaviour of the linear multilevel (i.e. p-nary) shift register from a knowledge of the shift register logical structure. The first method utilizes the relationship between the shift register logical configuration and the generating function associated with its cycle structure. The method is accordingly called as ' generating function method '. The second method makes use of the C_k - transform and associated linear recurrence concept (discussed in Chapter 1 with reference to linear binary sequences). These procedures are quite analogous to those considered in the binary situation in Chapter 1. However, the analysis of sequential behaviour of p-nary shift registers is considered here separately, because of the reason that the structural properties of the p-nary feedback shift registers ($p > 2$ and prime) differ from the structural properties of the corresponding binary sequences ($p=2$).

3.4.1 Use of generating function concept for the evaluation of null sequences associated with a given p-nary delay polynomial

Referring to the linear autonomous p-nary nth degree feedback shift register shown in Fig.(3.1), it is seen that eventhough 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 network is that for which $[F(D)]$ C equals zero, where F(D) is the p-nary characteristic delay polynomial of the autonomous network. This natural response C is hence called a null sequence associated with the delay polynomial F(D). The null sequence of a delay polynomial is thus periodic with a period N which depends on the system configuration and initial state. A delay polynomial may have several distinct null sequences. These null sequences are also called the solutions of the polynomial F(D).

It is of present interest to extend the classic idea of generating function to the p-nary situation to obtain all the null sequences of a given delay polynomial.

The theory states that a generating function G(x) may be associated with the null sequence of a delay polynomial F(D). An explicit expression for G(x) in terms of F(D) and the initial state of the corresponding shift register has been well developed for the binary case (Chapter 1, eqn. (1.14)). This means, given the polynomial F(D), (i.e. the logical structure of the p-nary shift register) and the initial state, the corresponding G(x) and hence the null sequence (cycle structure) can be evaluated. For this purpose, an expression for G(x) befitting the p-nary case will be at first developed in terms of the initial state, and the polynomial F(D) of the shift register.

Consider a p-nary sequence C represented by the successive terms (c_o, c_1, ... c_r) as the logical output of the mod-p adder (i.e. input sequence to the first stage) of the shift register of Fig. (3.1). We may associate a generating function G(x) with the sequence C and write :

$$G(x) = +\sum_{r=0}^{\infty} c_r x^r \qquad \ldots \qquad \ldots \qquad (3.5)$$

(The sign + stands for mod-p addition)

From the configuration of the shift register and nature of feedback, any term c_r in the sequence C is a modulo-p sum of the contents at the (r - 1)st state. Hence, the entire sequence C satisfies a linear recurrence relation of the form :

$$c_r = +\sum_{i=1}^{n} a_i c_{r-i} , \qquad \ldots \qquad \ldots \qquad (3.6)$$

where the coefficients, 'a_i' may assume any value in the modular field of integers 0, 1, 2, ... , p-1.

Assuming the initial state of the feedback shift register as (c_{-1}, c_{-2} , ..., c_{-n}) and substituting for c_r, eqn. (3.5) may be reduced to the form :

$$G(x) = \frac{+\sum_{i=0}^{n-1} b_i x^i}{1 - \sum_{i=1}^{n} a_i x^i} , \quad \text{(' - ' in the denominator stands for mod-p subtraction)}$$

$$\ldots \qquad (3.7)$$

where $$b_j = \sum_{i=1}^{n-j} a_{i+j} c_{-i} , \qquad 0 \leq j \leq n - 1.$$

In accordance with the modulo-p arithmetic, stated in brief in Section 3.3, G(x) may be written as :

$$G(x) = \frac{+\sum_{i=0}^{n-1} (p-1)(b_i D^i)}{F(D)} \quad x \qquad \ldots \qquad \ldots \qquad (3.8)$$

with $a_o = (p-1)$, and $I = D^o = 1$ as the identity operator and the symbol D^i corresponding to a delay of i digits.

Further, the given p-nary shift register may be activated from any of the $p^n - 1$ nonzero initial states. In case, the initial state is :

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

then, G(x) reduces to its simple form as :

$$G(x) = \frac{a_n(p-1)}{F(D)} \quad x \qquad \ldots \qquad \ldots \qquad (3.9)$$

Thus, in case the initial state and the logical structure of the shift register is specified, it is possible to find G(x) and hence the p-nary null sequence (cycle structure) generated by the multilevel feedback shift register. The period of the null sequence evidently depends on the initial state and the type of the delay polynomial of the shift register.

The sequential behaviour of the p-nary feedback shift register is studied here by classifying the delay polynomials, that characterize the sequential behaviour, as under :

A : Irreducible and primitive delay polynomials

B : Irreducible and nonprimitive delay polynomials.

C : Factorable delay polynomials.

If the given polynomial is primitive, the theory states that the period of its null sequence is maximum and equals $(p^n - 1)$ digits. Such a sequence is called a maximum length p-nary null sequence. Thus for a given primitive polynomial, the null sequence yielded by the corresponding generating function describes all the $p^n - 1$ distinct p-nary states of the shift register and constitutes the complete solution of the polynomial.

However, if the given polynomial is irreducible but nonprimitive, with any assumed initial state, the generating function describes a null sequence of nonmaximal length($<p^n - 1$ digits). As a result, a given polynomial of this class, will have several null sequences. But the theory states that an irreducible polynomial exhibits sequences of equal period. If C_1 is a null sequence of the polynomial and is of period N_1, the $(p^n - 1) / N_1$ null sequences of the polynomial constitutes the complete solution of the polynomial. To realize the set of sequences other than C_1 (already obtained from G(x)), we may proceed as follows -

We may consider a new initial state that is not described by the first sequence C_1, and repeat the method to arrive at

the second distinct null sequence C_2. This procedure may be continued until the $(p^n - 1) / N_1$ distinct null sequences are obtained. Such a method involves a lot of computation. A better method than the above is to make use of the following theorem :

If F(D) is a linear p-nary nth degree delay polynomial of an autonomous shift register, and if a sequence C of period N is a null sequence of F(D), then the sequences, C_i, given by -

$$C_i = (C + k D^q C) \qquad \text{(modulo-p addition)} \quad \ldots \quad (3.10)$$

where q is an integer in the range 1 to N, and k is a scalar multiplier in the range 1 to p-1, describes all the null sequences associated with the given polynomial.

Therefore, for permissible values of k and q, C_i describes null sequences of F(D). However, with only certain values of k and q , we realize distinct null sequences. Whether a selected set of k and q gives a new null sequence may be seen by carrying out the mod-p addition of the sequences C and k $D^q C$ for the first n digits and examining the resulting n digit p-nary number. If this has already appeared in the first sequence C_1 (say), no new sequence will be obtained. If not, another distinct sequence C_2 (say) of F(D) results from the mod-p addition. This procedure may be persuaded till all the

$(p^n - 1) / N_1$ distinct null sequences are realized. Normally k may be assumed to be unity, and q varied in the allowable range. To facilitate quick evaluation, it may be noted from eqn. (3.10) that any linear (mod-p) combination of null sequences of a polynomial is again a null sequence of the polynomial. This means, if C_1 and C_2 are two null sequences of F(D), then

$$C_j = (k_1 C_1 + k_2 C_2), \quad \ldots \quad \text{(mod-p addition)} \ldots (3.11)$$

where k_1 and k_2 are integers in the range 1 to p - 1 describes null sequences of the polynomial F(D). Thus, new sequences can be formed from the linear-combination of the already obtained sequences.

Suppose that the given polynomial F(D) is factorable. In such a case, F(D) exhibits null sequences of different periods depending upon the nature of its factors. However, all these sequences can be evaluated by first obtaining a null sequence C_1 (say) from the generating function G(x) of eqn. (3.8) and then utilizing the expressions (3.10) and (3.11). Thus, it is possible, by this generating function approach, to evaluate the complete set of null sequences of a given delay polynomial irrespective of the class into which the polynomial falls. Furthermore, the sequences obtained by this method indicate whether the given polynomial is primitive, or irreducible but nonprimitive, or factorable (mod-p).

An example, under each class of the polynomials, is given below :

Example 3.1 : (A case of primitive polynomial)

Consider the quadratic, quinary - delay polynomial given by -

$F(D) = 4 + 2D + 2D^2$, (p = 2, p = 5, mod-5 addition)

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

Assuming the initial state as '01' the corresponding generating function, from eqn. (3.9), is :

$$G(x) = \frac{2(5-1)}{4 + 2D + 2D^2}\, x, \qquad (\text{since } a_2 = 2)$$

$$= x\,(2 + 4D + 2D^2 + 2D^3 + 3D^4 + D^6 + 2D^7 + D^8 + D^9 + 4D^{10} + 3D^{12} + D^{13} + 3D^{14} + 3D^{15} + 2D^{16} + 4D^{18} + 3D^{19} + 4D^{20} + 4D^{21} + D^{22} + 2D^{24} + 4D^{25} + \ldots)$$

Hence, the null sequence C of F(D) is given by -

C : 2 4 2 2 3 0 1 2 1 1 4 0 3 1 3 3 2 0 4 3 4 4 1 0, 2 4 ..etc.

Clearly, the sequence C is cyclic with period $N = 24 (= 5^2 - 1)$ digits. Since the sequence C describes all possible nontrivial states of the quadratic, quinary shift register, we have obtained complete solution for the given polynomial. The polynomial is evidently a primitive one (mod-5).

Example 2 : (A case of irreducible and nonprimitive polynomial)

Consider the delay polynomial written as :

$F(D) = 4 + 3D + D^2$ (mod-5 addition)

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

With initial state '01', the generating function G(x) from eqn. (3.9) is :

$$G(x) = \frac{(1).(4)}{4 + 3D + D^2}\, x, \quad (\text{since } p = 5 \text{ and } a_2 = 2)$$

$$= x(1 + 3D + 3D^3 + 4D^4 + 4D^6 + 2D^7 + 2D^9 + D^{10} + D^{12} + 3D^{13} + \ldots).$$

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

C_1 : 1 3 0 3 4 0 4 2 0 2 1 0, 1 3 ... etc.

The sequence C_1 of period $N_1 = 12\,(5^2 - 1)$ digits and hence is a nonmaximal sequence. To obtain other solutions of F(D), we now utilize expression (3.10): With k = q = 1, we get the second distinct null sequence C_2 as under :

C_1 : 1 3 0 3 4 0 4 2 0 2 1 0, ... (repeats)
DC_1 : 0 1 3 0 3 4 0 4 2 0 2 1, ... (repeats)
C_2 : 1 4 3 3 2 4 4 1 2 2 3 1, ... " (mod-5 addition)

Sequences C_1 and C_2, of period 12 digits, describe all the $(5^2 - 1) = 24$ distinct states of the 2nd degree quinary shift register and thus constitute the complete solution of F(D). Since their periods are equal, F(D) is irreducible & nonprimitive.

Example 3 : (A case of factorable polynomial)

Consider the delay polynomial given by :

$F(D) = 4 + 4D + 2D^2$, (mod-5 addition)

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

With the initial state 01, the corresponding generating function G(x), from eqn. (3.8) gives the sequence C_1 given by :

C_1 : 2 3 1 0, 2 3 ... etc.

From eqn. (3.10), with k = q = 1, we get a second distinct sequence C_2 of F(D) as :

$C_2 = (C_1 + DC_1)$ = 2 0 4 1, ... of period 4 digits.

Utilizing expression (3.11), all the rest of the sequences of F(D) are determined and written below :

$C_3 = C_1 + C_2$: 4 3 0 1, ... of period 4 digits.
$C_4 = C_2 + C_3$: 1 3 4 2, ... " " "
$C_5 = C_2 + C_4$: 3 3 3 3 ... " 1 "
$C_6 = C_2 + C_5$: 0 3 2 4, ... " 4 "
$C_7 = C_4 + C_6$: 1 1 1 1 ... " 1 "
$C_8 = C_5 + C_7$: 4 4 4 4 ... " 1 "
$C_9 = C_5 + C_8$: 2 2 2 2 ... " 1 "

$\therefore$ period of sequences C_1 to C_9 = 24 = $(5^2 - 1)$ digits. And the set of sequences C_1 to C_9 constitutes compute solution of F(D).

3.4.2 Use of C_k-transform for the evaluation of null sequences of a given polynomial

In this section, the use of C_k-transform and associated linear recurrence (as discussed in Chapter 1) is emphasized in evaluating all the null sequences of a given delay polynomial, that describes the sequential behaviour of the linear p-nary nth degree feedback shift register shown in Fig. (3.1).

The characteristic equation of the autonomous linear shift register is given by :

$$\left[+ \sum_{i=0}^{n} a_i D^i \right] C = 0 \qquad \text{(mod-p addition)}$$

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

where a_i may assume any integer in the modular field (0, 1, 2, ... p - 1) and $a_o = (p - 1)$.

To find the null sequences of the polynomial F(D), similar to the binary case, we define a transform termed as C_k-transformed, as below :

$$\mathcal{C} (D^j C) = C_{k+j} \quad \cdots \quad \cdots \qquad (3.12)$$

where the symbol $\mathcal{C}$ 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 equation of the linear shift register may be written as :

$$C_k = a_1 C_{k+1} + a_2 C_{k+2} + \ldots + a_n C_{k+n} \quad \text{.. (mod-p addition)} \quad \ldots (3.13)$$

Or, using modulo-p arithmetic,

$$C_{k+n+1} = b_o C_{k+1} + b_1 C_{k+2} + \ldots + b_{n-1} C_{k+n} \quad \text{.. (3.14)}$$

where $b_i = \dfrac{(p - a_i)}{a_n}$, $(1 \leq i \leq n - 1)$ (mod-p reduction)

The linear recurrence stated in eqns. (3.13) and (3.14) may be utilized to evaluate all the null sequences of a given polynomial. If the polynomial is primitive - mod-p, for any nontrivial initial state, the sequence resulting from the above recursion algorithm will be seen to be of period $(p^n - 1)$ where n is the degree of the polynomial. However, as pointed out in the previous sub-section, for irreducible nonprimitive, and factorable polynomials, many null sequences exist. To evaluate the complete set of the distinct null sequences, we may have to either repeat the above recursion algorithm with proper selection of initial states of the corresponding shift register, or resort to applying the expressions (3.10) and (3.11). A case of primitive polynomial is illustrated in the following example by the C_k-transform and linear recurrence approach.

Example 3.4 : (A case of primitive polynomial)

Consider the characteristic equation of a second degree ternary feedback shift register given by :

$$(2 + 2D + D^2)\ C = 0 \qquad \text{(mod-3 addition)}$$

The $\mathcal{C}_k$-transformed version of the above equation from expression (3.14) becomes :

$$c_{k+2} = c_k + c_{k+1} \qquad \ldots \qquad \text{(mod-3 addition)}$$

or

$$c_{k+3} = c_{k+1} + c_{k+2}$$

Considering the set of terms (c_1, c_2) as representing the initial state (01) of the shift register, we may write all c_k's for $k > 2$, using the recursion formula (3.14), as follows :

With $k = 1 : c_3 = c_1 + c_2 = 0 + 1 = 1$ (mod-3 addition)

$k = 2 : c_4 = c_2 + c_3 = 1 + 1 = 2$

$k = 3 : c_5 = c_3 + c_4 = 1 + 2 = 0$

$k = 4 : c_6 = c_4 + c_5 = 2 + 0 = 2$

$k = 5 : c_7 = c_5 + c_6 = 0 + 2 = 2$

$k = 6 : c_8 = c_6 + c_7 = 2 + 2 = 1$

$k = 7 : c_9 = c_7 + c_8 = 2 + 1 = 0$

$k = 8 : 1_{10} = c_8 + c_9 = 1 + 0 = 1$

Since the last two c's (i.e. c_9 and c_{10}) represent the initial state '01', we stop persuading the recursion

The null sequence of the given polynomial is, therefore,

$$C : \underset{(c_8}{1}\ \underset{c_7}{2}\ 2\ 0\ 2\ 1\ \underset{c_2}{1}\ \underset{c_1)}{0}, \ldots$$

where C represents the input sequence to the first stage of the shift register. Since the null sequence C obtained above describes all the distinct nonzero states of the given quadratic ternary feedback shift register, we have obtained complete solution for the given delay polynomial, which is evidently a primitive modulo-3.

3.5 DETERMINATION OF THE DELAY POLYNOMIAL FROM ITS NULL - SEQUENCE

This section deals with the determination of the delay polynomial from its null sequence, which need not be maximal. Three methods are discussed here for this purpose. The first method determins the polynomial by mere examination of the given sequence and it is accordingly called ' direct method.' The second method utilizes the relation between the delay polynomial and the generating function associated with the given sequence. Lastly the third method is based on the C_k-transformed and recursion algorithm stated in last section.

3.5.1 Determination of p-nary delay polynomial by direct method

Let $C = (c_o, c_1, \ldots c_r)$, be the given null sequence of period N, associated with a linear p-nary nth degree delay

polynomial F(D), whereby $[F(D)]\ C = 0$ stands for the characteristic equation of the corresponding feedback shift register. To find F(D) corresponding to a given maximum length p-nary sequence C, we may proceed as follows :

Consider two consecutive states of the system such that in the first-state, (say reference state), all p-nary digits except one are zero. Let c' be the p-nary value of the first digit in the next state of the shift register as shown below -

Two consecutive states	Stage number of shift register							
	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-p sum of the contents of several of the stages at the first state. We may, therefore, write the following equation in this case :

$$c' = a_i c_i \quad \ldots \quad \ldots \quad \ldots \quad (3.15)$$

where a_i is the coefficient of D^i in the delay polynomial F(D), and ($1 \leq i \leq n$). Since c' and c_i are known from the given sequence, the p-nary coefficient a_i may be found. Thus, by considering n pairs of such consecutive states of the shift register, it is possible to evaluate all the p-nary feedback coefficients $a_1, a_2, \ldots a_n$ of the required delay

polynomial F(D).

The method assumes the occurrence of n states in the given p-nary sequence C, in which all digits except one are zero. This limitation poses no problem, since every p-nary m-sequence exhibits (p - 1)n states, each containing (n - 1) zeros and a non-zero digit. However, if a nonmaximal null sequence is given, which does not describe the said n states then, the generating function method or the C_k-transform method must be utilized to determine the polynomial. An example by direct method now follows -

Example 3.5 : (A case of m-sequence)

Consider the m-sequence C, given below, for which the corresponding delay polynomial is to be determined -

C : 2 0 2 1 2 2 1 0 2 2 2 0 0 1 0 1 2 1 1 2 0 1 1 1 0 0, ...

Clearly, the sequence C is ternary ; i.e. p = 3. Its period, N = 26 digits. As the sequence describes all the possible nonzero ternary states of a 3rd degree shift register, the degree of the corresponding delay polynomial is 3.

Thus, the polynomial may be expressed as :

$$F(D) = 2 + a_1 D + a_2 D^2 + a_3 D^3 \qquad .. \qquad (p = 3)$$

To determine the coefficients a_1, a_2 and a_3, the following states are considered :

Two consecutive states	Stage number of shift register								
	For a_1			For a_2			For a_3		
	1	2	3	1	2	3	1	2	3
Reference state	2	0	0	0	1	0	0	0	1
Next state	0	2	0	1	0	1	2	0	0

Making use of eqn. (3.15), the coefficients a_1, a_2, a_3 are found to be -

$a_1 = 0$, $a_2 = 1$ and $a_3 = 2$

Therefore, the delay polynomial corresponding to the given ternary m-sequence is :

$F(D) = (2 + D^2 + 2D^3)$.

It may be possible to apply this direct method and determine the polynomial of a certain nonmaximal sequence, despite the fact that it does not describe the required n states, each having (n - 1) zeros and a nonzero digit. However, in such a case, the solution to the problem will not be unique. This is illustrated by the following example :

Example 3.6 : (A case of nonmaximal null sequence)

Given the null sequence C as -

C : 2 0 0 1 0 0, ... (repeats)

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

The sequence C : 200100,... is ternary, i.e. p = 3. Its period N = 6 digits. This means the given sequence is nonmaximal, since $3^n - 1 \neq 6$ for any n. Further, in view of the fact that N = 6, the degree of the ternary shift register must be atleast 4, i.e. n = 4.

We may, therefore, represent the required polynomial as -

$$F(D) = (2 + a_1D + a_2D^2 + a_3D^3 + a_4D^4), \quad (\text{since } p = 3).$$

In the given sequence, there are two distinct states, each having (n - 1) zeros and a non-zero digit. From these two states, two of the four feedback coefficients may be determined. As shown below, the other two coefficients can also be obtained by suitably choosing the consecutive states.

Two consecutive states	Stage number of shift register											
	For a_2				For a_3				For a_1 & a_4			
	1	2	3	4	1	2	3	4	1	2	3	4
Reference state	0	1	0	0	0	0	1	0	1	0	0	2
Next state	0	0	1	0	2	0	0	1	0	1	0	0

Making use of eqn. (3.15), the coefficients are as follows -

$$a_2 = 0, \quad a_3 = 2 \quad \text{and} \quad a_1 + 2a_4 = 0 \quad (\text{mod-3 addition})$$

$$\text{i.e. } a_1 = a_4 = 1$$

OR

$$a_1 = a_4 = 2, \text{ since } p = 3$$

Hence $F(D) = (2 + D + 2D^3 + D^4)$

OR

$= (2 + 2D + 2D^3 + 2D^4)$.

3.5.2 Use of generating function in determining the p-nary delay polynomial from its null sequence

From the analysis of Section (3.4.1) , the generating function G(x) associated with the null sequence C of a linear p-nary nth degree shift register is related to the delay polynomial of the register by the eqn.(3.9) , which is rewritten below for convenience -

Assuming the initial state as -

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

$$G(x) = \frac{a_n(p-1)}{F(D)}\, x$$

Each cycle of the null sequence of the polynomial F(D) as described by the generating function G(x) ends with the assumed initial state appearing in the reverse order. (i.e. 0 0 .. 0 1 as 1 0 . . . 0 0) . Hence, we may find the polynomial F(D) from its null sequence C from the above equation, where G(x) is now written after arranging the given sequence C such that it ends with a 1 followed by (n - 1) zeros, in view of the above assumed initial state. The method is applicable to maximal as well as nonmaximal sequences. Two examples, one concerning an m-sequence and the other concerning nonmaximal sequence, are illustrated below.

Example 3.7 : (A case of maximal polynomial)

Given the null sequence C as -

C : 2 0 2 1 1 0 1 2, ... repeats

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

The sequence C is ternary i.e. p = 3. Its period is 8 digits. Further, the sequence describes all the $3^2 - 1$ nonzero states of a second degree shift register. Thus, the degree of the delay polynomial corresponding to C should be 2.

Hence,

$$F(D) = 2 + a_1 D + a_2 D^2.$$

Further, arranging the given sequence such that each cycle ends with a 1 followed by n - 1 = a zero, C appears as -

C : 1 2 2 0 2 1 1 0, ... (repeats)

Since the sequence is cyclic, we need to consider only one period. Thus the generating function for the cycle written above reads as :

$$G_1(x) = x (I + 2D + 2D^2 + 2D^4 + D^5 + D^6)$$

and from eqn. (3.9), the delay polynomial corresponding to C is :

$$F(D) = (2 + 2D + 2D^2).$$

To check the results, it may be verified that -

$$[F(D)]C = 0$$ (i.e. all zero sequence)

Example 3.8 :(A case of nonmaximal sequence)

Given the null sequence C as -

C : 2 0 0 1 0 0, ... etc.

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

The sequence C is here ternary ; i.e. p = 3. Its period is 6 digits. Hence, the degree of the required polynomial should be at least 4, i.e. n = 4. Further, in this case, any permissible values of k and q will not yield a null sequence with n - 1 = 3 zeros. However, we can still solve the problem with the help of the general expression for generating function given in equation (3.8) of Section 4.1. repeated below -

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

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

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

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

Considering only one cycle of the null sequence, we have -

$$G_1(x) = d_o + d_1 x + d_2 x^2 + \ldots + d_{N-1} x^{N-1} \quad \ldots \quad (3.16)$$

Expanding the general expression for G(x) in eqn.(3.8)-

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

$$d_1 = (b_1 + b_o a_1) = \left(\sum_{i-1}^{n-1} a_{i+1} c_{-i} + a_1 \sum_{i=1}^{n} a_i c_{-i} \right)$$

$$d_2 = b_2 + b_1 a_1 + b_o (a_2 + a_1^2)$$

. . . . . .

. . . . . .

and $d_r = b_r + \sum_{i=0}^{r-1} a_{r-i} d_i$ where $d_o = b_o$ ... (3.17)

we now proceed to solve the present example -

Sequence given = 2 0 0 1 0 0, ...

Writing the generating function of the sequence for one period, we get -

$$G_1(x) = (2 + x^3)$$

Comparing the coefficients of $G_1(x) = (2 + x^3)$ with the coefficients of $G_1(x)$ given in eqn. (3.16), we see that -

$d_o = 2$, $d_1 = 0$, $d_2 = 0$, $d_3 = 1$, $d_4 = 0$ and $d_3 = 0$

As already pointed out, the null sequence given by G(x) ends with the initial condition in reverse order.

Thus the initial state in this case is as shown below :

$$C : \underset{c_{-4}}{2} \quad \underset{c_{-3}}{0} \quad \underset{c_{-2}}{0} \quad \underset{c_{-1}}{1} \quad 0 \quad 0, \ \ldots$$

Substituting the initial conditions in dr, r = 0 to 2, we get the following equations :

$$a_3 = 2$$

$$2a_1 + a_4 = 0$$

$$a_1 a_4 + (a_2 + a_1^2) a_3 = 0 \qquad \text{(mod-3 addition)}$$

Solving the above equations in accordance with mod-3 arithmetic, the required polynomial is :

$$F_1(D) = 2 + D + 2D^3 + D^4 \qquad (\text{with } a_1 = a_4 = 1)$$

OR

$$F_2(D) = 2 + 2D + 2D^3 + 2D^4 \qquad (\text{with } a_2 = a_4 = 1)$$

3.5.2 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 a given null sequence making use of C_k-transform and associated linear recursion algorithm.

Let $C = (c_1, c_2, \ldots c_r)$, be the given null sequence of period N, associated with a linear p-nary nth degree delay polynomial F(D), whereby $[F(D)]\ C = 0$ stands for the characteristic equation of the corresponding shift register.

From the analysis of Section (4.2), the C_k-transformed version of the characteristic equation (3.2) may be written in either of the forms stated below -

$$c_k = a_1 c_{k+1} + a_2 c_{k+2} + \cdots + a_n c_{k+n} \cdots \quad (3.13)$$

$$c_{k+n+1} = b_o c_{k+1} + b_1 c_{k+2} + \cdots + b_{n-1} c_{k+n} \cdots \quad (3.14)$$

where $b_j = \frac{(p - a_j)}{a_n}$, $\quad 1 \leq j \leq n-1$

Further, it is obvious that for this type of formulations, if the set of terms (c_{k+1} , c_{k+2} , ... , c_{k+n}) represents the present state, then it is possible to formulate both past and future states of the shift register with the help of the recursion formulae stated above. To find the polynomial F(D) corresponding to a given null sequence, we may, therefore, consider n states of the shift register, and write the corresponding n equation with the help of eqns. (3.13) and (3.14). Since the states are known, the coefficients a_1, a_2, ... a_n of the polynomial can be evaluated. An example by this method is given below :

Example 3.9 : (A case of maximal sequence)

Given the null sequence C as -

C : 1 2 2 0 2 1 1 0, ...

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

The sequence is ternary (p = 3). Its period is 8 digits. This means that the system is of second degree ($3^2 - 1 = 8$). We may, therefore, represent the required polynomial as -

$$F(D) = (2 + a_1 D + a_2 D^2)$$

This means the characteristic equation of the system is :

$$(2 + a_1 D + a_2 D^2) \quad C = 0$$

OR

$$C = a_1 D + a_2 D^2 \quad C \qquad \text{(mod-3 addition)}$$

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

$$c_k = a_1 c_{k+1} + a_2 c_{k+2}$$

If c_1 , c_2 (i.e. c_{k+1}, and c_{k+2} with k = 0) represent the present state of the system, then the following equations may be written -

$$c_o = a_1 c_1 + a_2 c_2 \qquad \text{(mod-3 addition)}$$

$$c_{-1} = a_1 c_o + a_2 c_1$$

If the initial state is considered as $c_1 = 0$ and $c_2 = 1$, then from the given sequence we see that $c_o = 1$ and

$c_{-1} = 2$. Substituting these values we get -

$a_1 = 2$ and $a_2 = 1$.

Thus the delay polynomial corresponding to the given ternary sequence is -

$F(D) = (2 + 2D + D^2)$

C_k-transform and associated linear recurrence is thus seen to be quite a convenient tool to solve such problems.

3.6 SOME PROPERTIES OF p-NARY DELAY POLYNOMIALS AND THEIR NULL SEQUENCES

From the results of the analysis so far carried out in the present chapter and what appears in the literature (references have been stated in the introduction of this chapter), some useful properties of p-nary delay polynomials and their null sequences are stated in this section.

(1) Polynomials of several types exist for every positive modulus p and n, the degree of the linear p-nary shift register and these may be classified based on their factorable features as :

A : Primitive polynomials
B : Irreducible and nonprimitive polynomials
C : Factorable polynomials.

(2) A polynomial F(D) of degree n has a complete set of null sequences if and only if a_n and a_o are prime to the modulus p, where F(D) is given by :

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

(3) The smallest positive integer k such that the polynomial F(D) divides $D^k - 1$ is called the period of the null sequence of F(D).

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

This statement implies that primitive (mod-p) polynomial of degree n has only one null sequence of period $p^n - 1$ digits. Since the largest possible period of the null sequence of a linear p-nary n-stage shift register is $p^n - 1$, the null sequence of a primitive polynomial is the maximum length null sequence. Accordingly the primitive polynomial is also known by the name 'maximal polynomial.' Table 3.2 below lists some maximal polynomials for p = 3, 5 upto n = 5, some of which have been treated in this chapter.

(5) The number of maximal polynomials for given degree n and modulus-p is : $M_p(n) = \phi(p^n - 1) / n$, where $\phi(k)$ is the Euler phi function defined by $\phi(k)$ = the number of integers $\leq k$ which are relatively prime to k.

Table 3.2 : Form of F(D) : $\sum_{i=0}^{n} a_i D^i$, with $a_o = p - 1$.

Degree of F(D) n	Maximal polynomial F(D)	Period in digits
2	$2 + 2D + D^2$	8
2	$2 + D + D^2$	8
3	$2 + D^2 + 2D^3$	26
3	$2 + D + 2D^3$	26
3	$2 + 2D + D^2 + 2D^3$	26
3	$2 + D + 2D^2 + 2D^3$	26
4	$2 + 2D^3 + D^4$	80
4	$2 + D + D^4$	80
4	$2 + D^3 + D^4$	80
4	$2 + 2D + D^4$	80
4	$2 + 2D + 2D^2 + D^3 + D^4$	80
4	$2 + 2D + D^2 + D^3 + D^4$	80
4	$2 + 2D + 2D^2 + 2D^3 + D^4$	80
4	$2 + D + D^2 + 2D^3 + D^4$	80
5	$2 + 2D^2 + D^3 + D^4 + 2D^5$	242
5	$2 + 2D + 2D^3 + 2D^4 + 2D^5$	242

Example : Consider a 4-stage ternary shift register such that $\phi(3^4 - 1) = 80$. $\phi(80) = 32$. Dividing by this by four, the number of maximal polynomials(for n = 4) is 8.

(6) An irreducible but nonprimitive modulo-p polynomial is one that has no factors but that it is a factor of $D^N - 1$ (mod-p subtraction) for some integer N less than $p^n - 1$, n being the degree of the polynomial.

Accordingly, the period of the null sequence of an irreducible nonprimitive p-nary delay polynomial is less than the maximum of $p^n - 1$ digits. As such, the null sequence of any nonprimitive polynomial is a nonmaximal sequence.

(7) The polynomial $D^m - 1$ divides the polynomial $D^n - 1$ (without remainder) if and only if m divides n.

(8) If the polynomial F(D) divides $D^s - 1$, then s is a multiple of the period of F(D).

(9) The period of an irreducible, mod-p, polynomial of degree n is a divisor of $p^n - 1$ and hence is prime to p.

(10) For any mod-p polynomial F(D),

$$[F(D)]^p = F(D^p)$$

Hence, also

$$[F(D)]^{p^m} = F(D^{p^m}) \quad \text{for any integer m.}$$

(11) If k is prime to the modulus p, then, the polynomial $D^k - 1$ (mod-p) contains no repeated factors.

(12) If F(D) is a prime polynomial of period k, then $D^k - 1$ contains F(D) exactly once as a prime factor (mod-p).

(13) If the period of an irreducible polynomial F(D) is k, then the period of $[F(D)]^j$ is kp^r where $p^{r-1} < j \leq p^r$, p being modulus.

(14) A complete set of null sequences of a polynomial F(D) of degree n and modulus p defines the polynomial upto a constant factor prime to p.

(15) Given a periodic sequence C of nonnegative integers less than a fixed prime p, then, there exists a unique polynomial F(D) (modulo-p) of minimal degree which has C as a null sequence, and any other polynomial which has C as a null sequence is divisible by F(D).

(16) For every polynomial of degree n, mod-p, the length of all its distinct null sequences must equal $p^n - 1$ digits.

(17) In a p-nary m-sequence, replacing every digit by its mod-p complement results in the same sequence, but for the phase shift which equals $(p^n - 1) / 2$ digits. The second half of any p-nary ~~half~~ m-sequence ($p > 2$) is the mod-p complement of its first half. This of course implies that the period of the sequence is even.

(18) For every maximum length p-nary sequence obtained from an n-stage p-level linear feedback shift register, there

exists a related n-stage shift register which will produce a reverse sequence. This reverse sequence is the original sequence read in the reverse order. The procedure for finding the reverse sequence shift register connections is as follows :

If an n-stage shift register has feedback connections from n, k, m ... etc. with feedback coefficients $a_n = 1$, a_k , a_m ... etc. , the reverse sequence shift register will have a feedback connections from the same stages n, n - k, n - m ... etc. with feedback coefficients 1, a_k, a_m, ... etc.

(19) For every polynomial of degree n, its null sequence C satisfies a linear recurrence relation -

$$c_r = \sum_{i=1}^{n} a_i c_{r-i} \qquad \text{(mod-p addition)}$$

where c_r is any term in the p-nary sequence Cand a_i are the coefficients of the polynomial that lie in the range of integers 0 to p - 1.

(20) By means of the linear recurrence stated in property 19 it is possible to evaluate all the null sequences of a given delay polynomial. Alternatively, given a p-nary null sequence realizable from a p-level linear shift register, the corresponding polynomial can be found using the linear recurrence relation.

(21) Every p-nary null sequence $C = (c_o, c_1, \ldots c_r, \ldots)$ may be expressed by the associated generating function as -

$$G(x) = \sum_{r=0}^{\infty} c_r x^r$$

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

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

(22) Given a delay polynomial and the initial stage of the corresponding shift register, all its null sequences can be evaluated by means of the generating function concept. Likewise, the delay polynomial that corresponds to a given null sequence can be found with the help of the generating function.

(23) The null sequence of a delay polynomial as described by the generating function G(x) always ends with the assumed initial state of the shift register in its reverse order.

(24) The concept of vector diagram, suggested by Golomb (1964) for the binary case, may as well be extended to the p-nary sequences as outlined below.

A linear, autonomous p-nary nth degree shift register may be thought of as a device which takes any input vector

$(c_{k+1}, c_{k+2} \ldots, c_{k+n})$ and computes an output vector $(c_k, c_{k+1}, \ldots, c_{k+n-1})$. This means if the set of terms $(c_{k+1}, c_{k+2}, \ldots, c_{k+n})$ stands for the present state, then the immediate future state is given by the set of terms $(c_k, c_{k+1}, \ldots, c_{k+n-1})$. The table below shows how successors as well as predecessors are assigned by the multistable system assuming the set of terms $(c_{k+1}, c_{k+2}, \ldots c_{k+n})$ as representing input vector at the present. The period of the null sequence is taken as 'N' and p any prime integer > 2.

Table 3.3 :

	Stage number				
	1	2	...	(n-1)	n
	c_{k+N}	c_{k+N+1}	...	$c_{k+N+n-2}$	$c_{k+N+n-1}$
	c_{k+N-1}	c_{k+N}	...	$c_{k+N+n-3}$	$c_{k+N+n-2}$
Predecessors	....	....	...	....	....
	....	....	...	....	....
	c_{k+2}	c_{k+3}	...	c_{k+n}	c_{k+n+1}
(Present input vector) →	c_{k+1}	c_{k+2}	...	c_{k+n-1}	c_{k+n}
	c_k	c_{k+1}	...	c_{k+n-2}	c_{k+n-1}
	....	....	...	....	....
Successors	....	....	...	....	....
	c_{k-N+3}	c_{k-N+4}	...	$c_{k-N+n+1}$	$c_{k-N+n+2}$
	c_{k-N+2}	c_{k-N+3}	...	c_{k-N+n}	$c_{k-N+n+1}$

If the present input vector is represented by the symbol $[c_{k+1}]$, then we may depict the contents of Table (3.3) in the formof a diagram, which is called the 'Vector diagram', as shown in Fig. (3.3). The following may now be stated with reference to this vector diagram :

(a) The cycles in the vector diagram have no branch points.

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

(c) Predecessors or successors of vectors are unique.

(d) Distinct vectors have distinct successors.

(e) The second half of the vector diagram is the (modulo-p) complement of the first half respectively.

(25) For a given n, every p-nary m-sequence is pseudo-random in the sense that it satisfies the following three randomness properties :

(a) The Balance Property : Every p-nary consists of p-kinds of digits (i.e. 0s, 1s, 2s, ..., (p-1)s); and is of period equal to $(p^n - 1)$ digits. In each period the number of digits of every non-zero kind differs from the number of digits of zero-kind by 1. This implies that each non-zero p-nary digit appears (p^{n-1}) times and the zero-digit appears $(p^{n-1} - 1)$ times in each cycle of the sequence.

(b) The Run Property : The total number of runs of a p-nary m-sequence equals $(p - 1)(p^{n-1})$. These runs are equally distributed

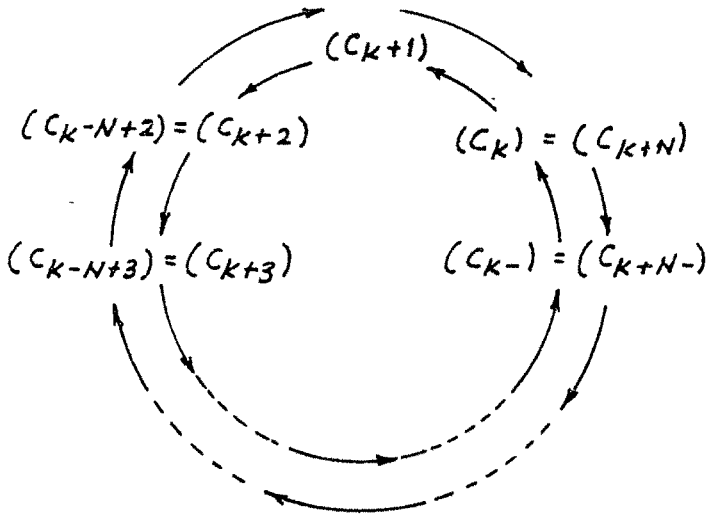


FIG. 3·3 VECTOR DIAGRAM FOR THE AUTONOMOUS SYSTEM OF TABLE 3·3

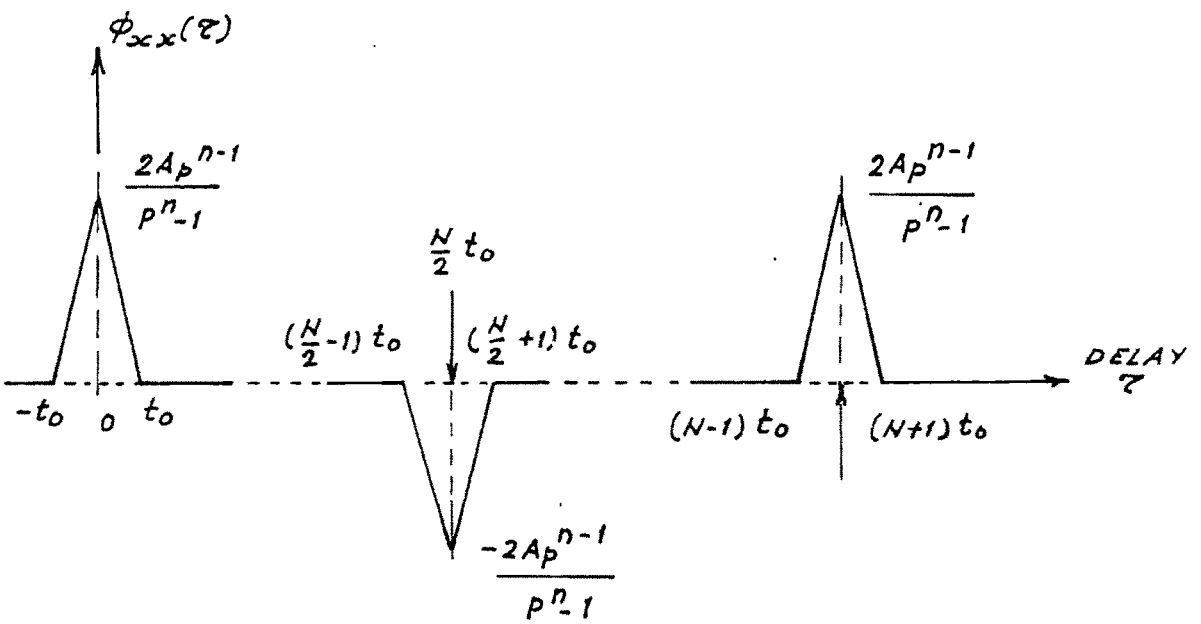


FIG. 3·4 AUTOCORRELATION FUNCTION OF A SIGNAL CORRESPONDING TO P-LEVEL m-SEQUENCE OF LENGTH $N = p^n - 1$ $(p > 2)$

among all the kinds of digits (including the zero-kind). Thus each kind has $(p-1)p^{n-1}/p = (p-1)p^{n-2}$ runs ($n > 2$).

(c) The Correlation Property : For every p, prime, ($p > 2$), the m-sequence is always antisymmetric in the sense that the second half of the sequence is the modulo-p complement of the first half. This of course implies that the period of the m-sequence is even. In mathematical terms, the second half of a p-level m-sequence signal X(t) is given by -

$$X(t) = - X(t + \frac{1}{2}N\, t_o)$$

where t_o is the clock-pulse period and N, the period of the m-sequence. Thus the second-order auto correlation function of a p-level m-sequence C is given by -

$$\phi_{cc}(s) = \frac{1}{N} \sum_{s=1}^{N} c_r c_{r+s}$$

$$= \frac{2A.p^{n-1}}{p^n - 1} \quad , \qquad s = 0,\ N,\ 2N \ \ldots$$

$$= - \frac{2A.p^{n-1}}{p^n - 1} \quad , \qquad s = N/2,\ 3N/2,\ \ldots$$

$$= 0 \quad , \qquad \text{elsewhere}$$

where

$$A = 1^2 + 2^2 + 3^2 + \ldots + \left(\frac{p-1}{2} \right)^2$$

The continuous autocorrelation function of the p-level signal X(t) is shown in Fig. (2.4).

(26) Every p-nary m-sequence exhibits the shift and subtract property which states that for all $s \not\equiv 0 \pmod{N = p^n-1}$ is the period of the m-sequence C) there exists an integer w such that -

$$C \ominus D^s C = D^w C \quad , \qquad \text{for } 1 \leq s, w \leq N - 1$$

(27) Any linear combination of null sequences of a polynomial is again a null sequence of the polynomial.

(28) Given an n-stage p-nary linear shift register and (2n - 1) digits of a required m-sequence, it is possible to determine uniquely the feedback connections of the shift register. 2n digits are required, since n digits are needed as an initial condition, and n additional digits are necessary to specify uniquely the feedback coefficients.

(29) If a p-nary m-sequence is sampled with f equal to a power of p then the same sequence results.

(30) Sampling a p-nary m-sequence with each f in turn, $(f, p^n - 1) = 1$, $1 \leq f \leq p^n-2$, will produce all p-nary m-sequences of period $p^n - 1$ (each n times) and no others. It may be noted that the number of different m-sequences of period $p^n - 1$ is $n^{-1}.\phi(p^n - 1)$.

(31) If in any p-nary m-sequence of period $p^n - 1$, we replace the nonzero terms by zero and zero terms by one, then,

the resulting binary sequence has period $p^n - 1 / p - 1$ and is pseudo-noise.

(32) If it is known that a periodic p-nary m-sequence is a maximum length sequence for some polynomial, then, it is easy to examine the sequence and determine the polynomial itself. (See example 3.5).

(33) Given the irreducible polynomial -

$$F(D) = + \sum_{i=0}^{n} a_i D^i \qquad \text{(mod-p addition)}$$

Let $F_1(D) = + \sum_{i=0}^{n} a_i D^{n-i}$, then $F_1(D)$ is also irreducible. In fact, the sequences of $F(D)$ and $F_1(D)$ are time inverse of each other.

(34) A pseudorandom signal based on any p-nary m-sequence has the definitive characteristic reference phase that is uncorrelated with constant and linear signals; a property which is useful in system identification by means of crosscorrelation.

A reference phase $r(t)$ of a pseudorandom signal $s(t)$ is a translation of $s(t)$ defined by -

$$r(t) = s(t + \alpha)$$

with the particular properties

$$\int_0^T r(t)\,dt = 0 \quad \text{and} \quad \int_0^T t.r(t)\,dt = 0$$

(35) If a p-level m-sequence signal is the input to a nonlinear system in which the 2nd order kernal is the only even order kernal present, the measurement of the 2nd order kernel by crosscorrelation involves only the 4th order autocorrelation function properties of the signal.

The 4th order autocorrelation functionsare all different for different m-sequences of the same period due to the existence of linear relationships between members of the m-sequence which are dependent on the characteristic polynomial of the sequence.

3.7 GENERATION OF DELAYED REPLICAS OF LINEAR p-LEVEL MAXIMUM LENGTH SEQUENCES

It is shown that an m-sequence generated with an n stage linear p-level shift register with modulo-p feedback has a cycle length of $N = p^n - 1$ p-nary digits. The autocorrelation function of the signal x(t) corresponding to such an m-sequence is defined by -

$$\phi_{xx}(\tau) = \frac{1}{Nt_o} \int_{o}^{Nt_o} x(t - \tau).x(t)\,dt$$

where t_o is the digit period.

Where this property is of interest (e.g. System identification by crosscorrelation), copies of the same sequence with

various relative time delays are required. This section presents several methods of determining the p-level linear feedback shift register connections for providing the delayed versions of the basic m-sequence.

It is known that several techniques have been communicated for the determination of binary feedback shift register connections for delayed copies of binary m-sequences. (S.H. Tsao 1964, A.C. Davies 1965, 1965, 1968, B.Ireland and J.E. Marshall 1968, C.A. Stapleton 1971).

In view of this, the content of this section is divided into two parts. As the first part (Section 3.7.2) the presently available techniques (references listed above) for obtaining delayed copies of 2-level m-sequences are extended to cover the more general p-nary ($p > 2$ and prime) situation. (Methods 1 to 6 discussed below). As the second part of this section, (Section 3.7.3) a new method is described to determine the p-nary shift register connections for the realization of the delayed copies of the basic m-sequence. This new method makes use of the familiar concept of the generating function associated with the sequence. It will be seen that this method yields quick results as the only calculation involved here is simple modulo-p addition.

3.7.1 (Method 1) Direct-Method of obtaining delayed m-sequences

The characteristic equation of an n stage p level modulo-p feedback shift register is given by :

$$C = (a_1 D + a_2 D^2 + ... + a_n D^n)C \quad ... \quad (3.17)$$

where C represents the logical output sequence of the modulo-p adder and a_i (i = 1 to n) are the feedback coefficients.

If C is defined as the basic maximum length p-level sequence, then the delayed sequences DC to D^nC are readily available at the respective outputs of the register. It is, therefore, required to provide the delayed versions $D^{n+1}C$ upto D^NC where $Nt_o = (p^n - 1)t_o$ is the p-nary m-sequence repetetion period. One way of realizing the delayed copies of C is to add extra stages to the system. This method, although attractive from the view-point of synchronization of the various outputs, would be obviously wasteful specially where only a small number of selected delayed copies of the sequence are to be provided. In such situations, the shift and add property of m-sequences leads itself readily to the purpose of producing specially wanted delays with the help of mod-p adders as discussed below.

3.7.2 (Method 2) Shift and add property for obtaining delayed versions

Tsao (1964) has shown that phase delayed versions of binary m-sequences can be obtained by means of mod-2 adders in conjunction with the sequence generator (fsr) by making use of the shift and add property of the maximum length linear binary sequences. Since every p-level m-sequence, for p prime, exhibits the shift and add property, the delayed copies of a p-nary m-sequence may as well be provided utilising this property as shown below -

As before, if C is defined as a reference version of a given p-nary m-sequence and D^iC is the version of C delayed by a time it_o, then the digit-by-digit mod-p sum sequence is :

$$C + D^iC = D^kC, \qquad i \neq 0 \text{ and } N/2, \quad k \neq 0 \quad \ldots(3.18)$$

$$= D^{N/2}C, \qquad i = 0,\ i,\ k \text{ integers}$$

Now, for a p-level m-sequence generated by the n-stage linear shift register of Fig. (3.1),

N $n(p-1)$ delayed versions are available from the m-sequence generator,

$\frac{n(n-1)}{2}(p-2)^2$ delayed versions from combinations of outputs of two stages

$\frac{n(n-1)(n-2)}{3}(p-1)^3$ from combinations of output: of three stages

.....

.....

and $(p-1)^n$ from combinations of all the n stages.

Thus,

$$N = p^n - 1 = \sum_{r=1}^{n} n_{C_r} (p-1)^r \quad \ldots \quad (3.19)$$

This serves as a good remainder of how the whole gamut of delayed versions can be obtained in the p-nary situation. Further it is known that every p-nary m-sequence ($p > 2$ and prime) possesses an antisymmetric property in the sense that the second half of the sequence is the modulo-p complement of the first half. Hence we need only to provide the delayed versions from $D^{n+1}C$ upto $D^{N/2}C$, and the sequences $D^{N/2+1}C$ upto $D^{N}C$ may be obtained by complementing the sequences DC to $D^{N/2}C$ in the modulo-2 sense. Hence for generating all the delays, ($N/2 - n$) mod-p adders and ($N/2-1$) mod-p complementators are required. An example by this method now follows :

Example : 3.10

Given that the characteristic equation of a ternary shift register is :

$$(2 + D^2 + 2D^3)\, C = 0, \quad \ldots \quad \ldots \quad (3.20)$$

determine the shift register connections for delayed sequences.

The given system, being ternary and 3rd degree, generates an m-sequence of length $Nt_o = (3^3 - 1)t_o = 26t_o$, where t_o is the shift pulse period.

Representing the output of the feedback logic device by C, the m-sequences DC, D^2C and D^3C are readily available from the ternary shift register.

From the above characteristic equation,

$$D^4C = (2D + D^3)C \qquad D^9C = (D^2 + D^4)C$$
$$D^5C = (2D^2 + D^4)C \qquad D^{10}C = (2D^3 + D^6)C$$
$$D^6C = (2D + 2D^2)C \qquad D^{11}C = (2D^2 + D^8)C$$
$$D^7C = (2D^2 + 2D^3)C \qquad D^{12}C = (2D + D^2)C$$
$$D^8C = (D + D^3)C \qquad D^{13}C = (2D^2 + D^3)C$$
$$= (D^{N/2}C) \quad \ldots \quad (3.21)$$

(in the above equations ' + ' represents mod-3 addition).

Thus, ten (= N/2 - n) mod-3 adders are needed for generating delayed versions D^4C to $D^{13}C$. And, twelve (= N/2-1) mod-3 complementators (which will be merely invertors in case the ternary levels are chosen as 1, 0, -1) are required for providing the delays $D^{14}C$ upto $D^{26}C$.

It may be noted here, with the exception of D^5C, D^9C, $D^{10}C$ and $D^{11}C$, all the rest of the delayed versions upto $D^{13}C$ are realized by the first serial addition. And the versions 5th, 9th, 10th and 11th by the second serial addition.

Although the method is quite advantageous if only a small number of selected delayed copies are required, it has

the following drawbacks :

1. Each delayed version is obtained by a number of mod-p additions $\leq (n - 1)$.
2. Since all the delayed copies are not available in one serial addition, synchronization of the various outputs will be disturbed due to the finite speed of the mod-p adders and complementators.

So much so, the method is preferable when the required delays are rather scattered in terms of their relative delays.

3.7.3 (Method 3) Polynomial long-division technique

Davies (1965, 1968) presented a simple method for calculating the linear combination required to give a specified delayed version of a binary m-sequence. The method involves polynomial long division and is not restricted to short sequences. The extension of this method to the p-level m-sequence will now be considered.

It is evident that any linear combination of m-sequences of multistable feedback shift register is again an m-sequence of the register. Hence, any specified delayed version, say D^kC, may be written as :

$$D^kC = (k_1D + k_2D^2 + ... + k_nD^n) \qquad \text{(mod-p addition)}$$

where the coefficients $(k_1, k_2 ..., k_n)$ are again integers over the modular field GF(p).

Now, dividing the delay polynomial F(D) of the multistable shift register into D^k, the following equation may be obtained :

$$D^k = F(D).Q(D) + R(D) \quad \ldots \quad \ldots \quad (3.23)$$

where Q(D) is the quotient and R(D), the remainder polynomial (with no constant term) and of degree less than that of F(D).

According to equation (3.3)

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

Hence,

$$D^kC = [R(D)]C \quad \ldots \quad \ldots \quad (3.24)$$

comparing eqns. (3.22) and (3.24), it is clear that the coefficients of the remainder polynomial R(D) are the required coefficients k_1 to k_n. Since the degree of R(D) must be less than the degree of F(D).

Example: (3.11)

Given a 2nd degree quinary system described by the characteristic equation :

$$[F(D)]\ C = (4 + 2D + 2D^2)C = 0 \quad \text{(mod-5 addition)} \quad \ldots (3.25)$$

find an expression for the delayed version D^9C in terms of the outputs directly available from the multistable system.

Let, $D^9C = (k_1D + K_2D^2)C \quad \ldots \quad \ldots \quad (3.26)$

Now, the division of the above delay polynomial F(D) into D^9 may be carried out with detached coefficients as follows :

```
                9  8  7  6  5  4  3  2  1  <-- power of B
4  2  2 ) ------------------------------
          1
          1  1  2
             4  3
             4  4  3
                4  2
                4  4  3
                   3  2
                   3  3  1
                      4  4
                      4  4  3          (Division over
                            2             mod-5)
                         2  2  4
                            3  1 (remainder)
```

Therefore, the remainder polynomial is :

$$R(D) = 3D^2 + D$$

By equation (3.21)

$$D^9C = (D + 3D^2)C \qquad \text{(mod - 5 addition)}$$

which is the required result.

This method is evidently more simple and systematic and carries the distinct advantage that it can be used even for every long sequences as the only calculation required is the polynomial long division, which is a step by step process, readily performed on a digital computer with mod-5 logic.

3.7.4 (Method 4) Polynomial division method - an alternative solution

Davies (1968) presented another alternative solution by polynomial division technique to the problem of obtaining delayed versions. The statement of the problem as applied to p-level sequences is as follows :

Given the nth degree polynomial F(D), which generates a p-nary m-sequence the objective is to determine the least positive integer k satisfying an equation of the form :

$$D^k = k_1 D + k_2 D^2 + ... + k_n D^n \quad ... \quad (3.27)$$

where k_1 to k_n are known coefficients from GF(p) and where ' + ' denotes addition modulo-p.

The value of k may be determined by dividing F(D) into the right hand side expression of eqn. (3.27), and continuing the division until a single term remainder polynomial is obtained. This remainder is D^k. However, the division is to be carried out by writing the F(D) and the R.H.S. of eqn.(3.27) in ascending powers of D. The following example illustrates this technique.

Example 3.12

Given that $F(D) = 2 + D^2 + 2D^3$ (mod - 3 addition) and that, $D^k = D + D^3$, find k.

The division of F(D) into $(D + D^3)$ in accordance with mod-3 arithmetic is as shown below :

```
                  1  2  3  4  5  6  7  8     power of D ⟶
                ------------------------
2  0  1  2 ) 1  0  1
             1  0  2  1
             ---------
                2  2                        (mod-3 division)
                2  0  1  2
                ---------
                   2  2  1
                   2  0  1  2
                   ---------
                      2  0  1
                      2  0  1  2
                      ---------
                               1
```

The remainder is D^8, so k = 8.

It may be noted here that in both the methods 3 and 4 the whole division is to be performed to obtain the linear logic for each specified delayed-version of the m-sequence.

3.2.5 (Method 5) A practical method to determine multistable shift register connections for delayed m-sequences

Ireland and Marshall (1968) described a practical method to determine the modulo-2 shift register connections for producing delayed (or advanced) versions of a binary m-sequence. This method will now be considered in relation to p-nary m-sequences.

Given that the state (column) vector (Elspas 1959) of a given feedback multistable shift register is C_o at t = 0,

then, the state C_j after a time equal to j shift pulses is given by :

$$C_j = T^j C_o \quad \ldots \quad \ldots \quad (3.28)$$

where T is a constant n x n matrix with elements 0, 1,...,p-1, modulo-p arithmetic being used to simplify powers and products.

Defining the sense of C_o and C_j as ih Fig.(3.5) it is seen that the length of the basic sequence c_n, c_{n+1}, ..., equals $N = p^n - 1$ digits and the sequence c_{n+j}, c_{n+j+1},... is the sequence delayed by (N - j) elements or shifts.

Now, c_{n+j}, which is the first term in C_j is obtained by multiplying the first row of T^j with the column vector C_o. If this first row is known, the element c_{n+j} can be obtained.

Let the p-level shift register be set to the initial state (100....0). If a matrix ϕ_o is defined as shown in Fig.(3 then, the matrix ϕ_j can be expressed as

$$\phi_j = T^j . \phi_j$$

$$\text{Hence, } T^j = \phi_j \phi_o - 1 \quad \ldots \quad \ldots \quad (3.29)$$

Then, the required first rwo of T^j is given by the product of the first row of ϕ_j with the column of ϕ_o^{-1} in turn. Since the first row of ϕ_j represents the vector C_{j+n-1} (in the reverse order), only ϕ_o^{-1} is to be calculated for a given p-stable

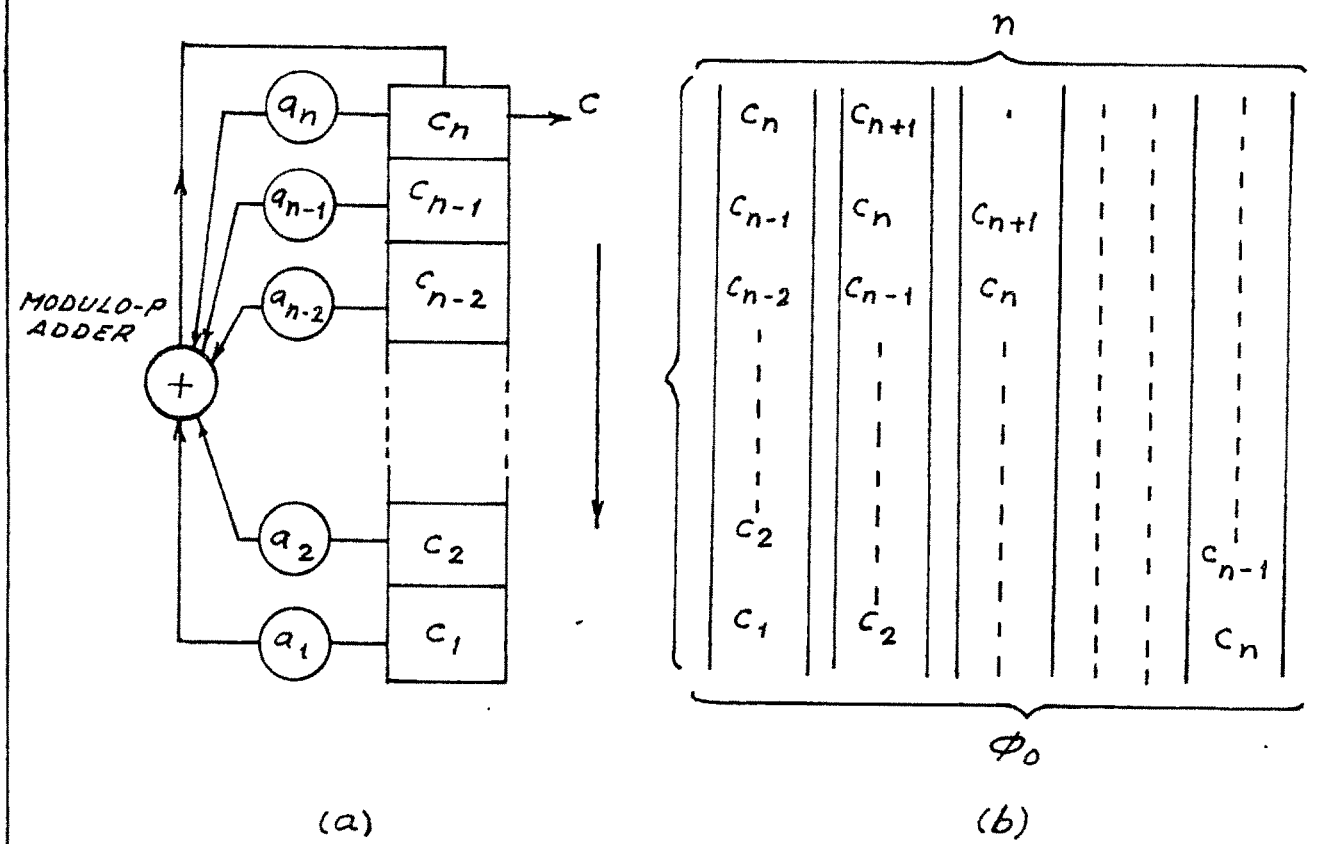


FIG. 3·5 (a) GENERATION OF DELAYED m-SEQUENCE USING MATRIX METHOD

(b) MEANING OF ϕ_0

shift register.

In short, the given multistable shift register is set up initially to $C_o = (1,00 \ldots 0)^t$, and shifted (j+n-1) times. The resulting state vector C_{j+n-1} written in the reverse order as a row vector, is then multiplied by ϕ_o^{-1}. The product yields finally a row vector, in which all non-zero elements (with p-nary values) give the shift register connections necessary to obtain the sequence advanced by j shifts. The following example illustrates the technique :

Example 3.7

Given that the characteristic equation of a ternary shift register is :

$[F(D)]\ C = (2 + D^2 + 2D^3)C = 0$, (mod-3 addition)

determine the shift register connections for the sequence advanced by 14 shifts.

The successive occurance of states is in the given shift register is shown in Table 3.4 below:

At time t = 0, the state vector (column) is :

$C_o = [1\ 0\ 0]^t$

By definition, (Fig. 3.5)

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

Hence,

$$\phi_o^{-1} = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$ (reduced as per mod-3 arithmetic)

For the m-sequence advanced by 14 shifts,

$$j = 14, \text{ Therefore, } C_{j+n+1} = C_{16} = [1\ 2\ 0]$$

(When written in reverse order) $C_{16} = [0\ 2\ 1]$

$$\text{And, } (C_{16}.\phi_o^{-1}) = [0\ 2\ 1] \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0\ 2\ 1]$$

Thus, the mod-3 sum of the outputs of the second stage (multiplied by 2), and the third stage yields the m-sequence advanced by 14 shifts, as may be verified from Table 3.

Table 3.4 Succession of states in the shift register

State No.	Stage No. 1	2	3	State No.	Stage No. 1	2	3
1	1	0	0	14	2	0	0
2	0	1	0	15	0	2	0
3	1	0	1	16	2	0	2
4	2	1	0	17	1	2	0
5	1	2	1	18	2	1	2
6	1	1	2	19	2	2	1
7	2	1	1	20	1	2	2
8	0	2	1	21	0	1	2
9	1	0	2	22	2	0	1
10	1	1	0	23	2	2	0
11	1	1	1	24	2	2	2
12	0	1	1	25	0	2	2
13	0	0	1	26	0	0	2

3.7.6 (Method 6) Delayed versions by employing requisite run-out stages

Recently Stapleton (1971) described an economical means of generating delayed binary m-sequences using an extended shift-register and an inversion of Davies' method of delay generation. The results obtained by this method in the case of a ternary shift register are tabulated below :

Table 3.5

Characteristic eqn. of the shift register : $(2 + D^2 + 2D^3)C = 0$
Period of the m-sequence C = 26 digits
Number of run-out stages provided : Two only
Delayed versions directly available: DC to D^5C
Form of delayed version, $D^kC = \sum_{i=1}^{5} k_i D^i C$ (mod-3 addition)

Delayed version, D^kC	Coefficients of D^kC				
	k_1	k_2	k_3	k_4	k_5
D^6C	2	2	0	0	0
D^7C	0	2	2	0	0
D^8C	0	0	2	2	0
D^9C	0	1	0	1	0
$D^{10}C$	0	0	1	0	1
$D^{11}C$	2	0	0	0	1
$D^{12}C$	2	1	0	0	0
$D^{13}C$	0	2	1	0	0

The delayed versions $D^{14}C$ to $D^{26}C$ are mod-3 compliment of the delayed version DC ... $D^{13}C$, Here all the delayed versions are obtained in one serial addition.

3.7.7 (Method 7) Use of generating function concept for the determination of p-nary shift register connections for delayed m-sequences

An attempt is made in the sub-section to present a simple method to determine p-nary shift register connections for the realization of the required delayed copies of the m-sequence. The method makes use of the familiar concept of generating function associated with the m-sequence (Golommb 1967). As the only calculation involved here is simple modulo-p addition, it can provide quick results.

Before considering the method, it is necessary to recall the following four properties of a p-nary m-sequence as generated by a linear n-stage p-level feedback shift register.

3.7.7.(a) Four Properties of p-nary m-sequences :

1. The m-sequence generated by the n-stage p-level feedback shift register (modulo-p feedback) is cyclic with a period $T = p^n - 1$ clock pulse intervals.
2. There are $p^n - 1$ phase distinct m-sequences corresponding to each of the $p^n - 1$ possible nonzero initial states of the feedback shift register.
3. If an m-sequence C is operated by a polynomial $Q(D)$ in D (with its coefficients over the modular field of integers 0 to p - 1), a phase-shifted version of the sequence C results.

4. For $p > 2$ and prime, the second half of every p-nary m-sequence is the modulo-p complement of the first half.

3.7.7(b) Determination of feedback connections for delayed m-sequences

It is a familiar fact every feedback shift register m-sequence $C = \{c_r\}$ satisfies a linear recurrence relation

$$c_r = \sum_{i=1}^{n} a_i c_{r-i} \qquad \ldots \qquad \ldots \qquad (3.30)$$

where a_i assumes a value in the modulo field of integers 0 to p - 1.

A close look at the methods of studying linear recurring sequences reveals that a generating function G(x) may be associated with the p-level m-sequence as under :

$$G(x) = \sum_{r=0}^{\infty} c_r x^r \qquad \ldots \qquad \ldots \qquad (3.31)$$

Assuming the initial state of the feedback shift register as :

$$c_{-1}, c_{-2}, \ldots\ldots, c_{-n}$$

and making use of the linear recurrence stated in eqn.(3.30), the generating function G(x) has been shown in Section (3.4.1) to be of the form : (eqn. 3.8 rewritten below).

$$G(x) = \frac{\sum_{i=0}^{n-1} (p-1) b_i x^i}{\sum_{i=0}^{n} a_i x^i}, \quad a_o = p - 1,$$

where

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

Identifying the denomenator of the above equation with the characteristic delay polynomial F(D) of the shift register, G(x) may be written as :

$$G(x) = \left[\left\{ \sum_{i=0}^{n-1} b_i D^i \right\} \frac{p-1}{F(D)} \right] x \quad \ldots \quad \ldots \quad (3.32)$$

It is apparent from eqn. (3.32) that there exists a duality between the characteristic polynomial F(D) and the generating function G(x). (i.e. the m-sequence under consideration). Under the circumstances, the term within the curly-brackets of the eqn. (3.32) may be made use of to determine the p-level shift register connections necessary for the realization of delayed versions of the m-sequence as discussed below :

With the initial state of the shift register given by

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

the generating function G(x) in eqn. (3.32) becomes:

$$G(x) = \frac{a_n (p-1)}{F(D)} x \quad \ldots \quad \ldots \quad (3.33)$$

How, if the m-sequence described by G(x) in eqn. (3.33) is considered as the reference sequence C, then, by property 3 of Section (3.7.7a), the m-sequences described by G(x) in eqn.(3.32)

under various initial conditions, are merely the delayed version of the reference sequence C. This means that the term within the curly brackets of eqn. (3.32) acts as a ' Delay Operator ' on the reference sequence.

This delay operator evidently depends on the initial state of the shift register and thus yields a distinct delayed version of the m-sequence C with each of the $p^n - 1$ distinct nonzero initial states of the register (property 2 of Sec.3.7.7a).

Therefore, if a relationship between the m-sequence described by the generating function G(x) and the initial state of the shift register is established, then, by merely substituting the initial conditions corresponding to a specified delayed sequence, the required delay operator or the shift register feedback connections for the generation of the specified delayed-version can be readily obtained. This relationship can be derived by considering the succession of states in the feedback shift register -

Succession of states in the shift register of Fig.(3.1)

State No.	m-sequence of length $p^n - 1$ digits				
	C	DC	D^2C	...	D^nC
First state	c_o	c_{-1}	c_{-2}	...	c_{-n}
Second state	c_1	c_o	c_{-1}	...	c_{-n+1}
Third state	c_2	c_1	c_o	...	c_{-n+2}
. . . . .	. . . . .				
. . . . .	. . . . .				
$(p^n - 2)$th state	c_{N-1}	c_{N-2}	c_{N-3}	...	c_{N-n-1}
$(N = p^n-1)$th state	c_N	c_{N-1}	c_{N-2}	...	$c_N - n$

since the period of the m-sequence equals N shift pulse intervals, it may be written that :

$$c_N = = c_o$$

$$c_{N-1} = c_{-1}$$

$$c_{N-2} = c_{-2}$$

$$\cdots\cdots\cdots$$

$$c_{N-n} = c_{-n}$$

It is clear from the above equations that the initial state $(c_{-1}, c_{-2}, \ldots . c_{-n})$ of the shift register appears at the end of the reference m-sequence C (logical output of mod-p adder of Fig.(3.1) in its reverse order.

Hence, by mere observation of the required delayed sequence, the corresponding initial state of the shift register can be noted, substitution of which in the curly bracketed term of equation (3.32) directly yields the shift register connections for the delay generation.

Specifically, the shift register connections for a given delayed version D^qC ($n < q < p^n - 1$) are given by

$$D^qC = \left[\sum_{i=0}^{n-1} \left(\frac{b_i}{a_n} \right) D^i \right] C \quad \ldots \quad \ldots \quad (3.34)$$

(Curly bracketed term of eqn.(3.32))

where,

$$b_j = \sum_{i=1}^{n-j} a_{i+j} \, c_{-i} \quad \ldots \quad \ldots \quad (3.35)$$

is evaluated with the initial conditions corresponding to the delayed version D^qC . Here, the coefficients b_i are to be divided by a_n because the elements of the reference m-sequence C have been previously multiplied by a_n (see eqn.(3.33)).

To clear the above ideas, an example is given below :

Example (3.14)

The characteristic equation of a quinary feedback shift register is given as -

$$[F(D)]\, C \doteq [4 + 2D + 2D^2]\, C = 0 \quad \text{(mod-5 addition)} \quad \ldots \quad (3.36)$$

Determine the feedback connections for $D^{13}C$.

As before, comparing the given characteristic equation with the general equation (3.3), we see that -

$$n = 2, \quad p = 5$$

and

$$a_o = 4, \; a_1 = 2, \text{ and } a_2 = 2 \qquad \ldots\ldots \qquad (3.37)$$

Starting with the initial condition (0 1), the reference m-sequence C (logical output of of the mod-5 adder) may be written :

C : 2 4 2 2 3 0 1 2 1 1 4 0 3 1 3 3 2 0 4 3 4 4 1 0, ...

Hence,

$D^{13}C$: 0 3 1 3 3 2 0 4 3 4 4 1 0 2 4 2 2 3 0 1 2 1 1 4, ...

Now, the initial conditions corresponding to the delayed-version $D^{13}C$ are the last two digits of the sequence taken in reverse order i.e.,

$$c_{-1} = 4 \text{ and } c_{-2} = 1$$

Substituting these initial conditions in the delay operator (eqn.(3.34)), we get -

$$D^{13}C = \frac{b_o + b_1 D}{a_2} C \qquad \ldots \text{ (mod-5 addition)}$$

where,

$$b_j = \sum_{i=1}^{n-1} a_{i+j} \, c_{-i} \qquad \ldots (n = 2)$$

Evaluating the coefficients b_j and b_1 with the help of eqns. (3.37) and (3.38)

$$b_o = a_1 c_{-1} + a_2 c_{-2}$$

$$= (2)(4) + (2)(1)$$

$$= 0 \qquad \text{(mod-5 reduction)}$$

$$b_1 = a_2 c_{-1}$$

$$= (2)(4)$$

$$= 3 \qquad \text{(mod-5 reduction)}$$

Hence, the delayed sequence $D^{13}C$ is given by :

$$D^{13}C = \frac{3}{2}DC = 4DC \qquad \text{(mod-5 reduction)}$$

Verification (mod-5 arithmetic)

C : 2 4 2 2 3 0 1 2 1 1 4 0 3 1 3 3 2 0 4 3 4 4 1 0, ...

DC : 0 2 4 2 2 3 0 1 2 1 1 4 0 3 1 3 3 2 0 4 3 4 4 1, ...

4DC : 0 3 1 3 3 2 0 4 3 4 4 1 0 2 4 2 2 3 0 1 2 1 1 4, ...

: $D^{13}C$

It may be noted that in the p-nary case ($p > 2$ and prime), it is only necessary to determine the shift register connections for delays from $D^{n+1}C$ to $D^{N/2}C$ ($N = p^n - 1$), as the connections for the delayed versions $D^{N/2+1}C$ upto $D^{N}C$ can be simply obtained by complementing the connections of the copies DC to $D^{N/2}C$ in the modulo-p sense (property 4 of Sec.3.7.7a).

The method is quite simple and provides quick results as the only calculation involved is simple mod-p addition.

3.8 A STRUCTURAL PROPERTY OF A p-NARY m-SEQUENCE

In this section, a structural property of the maximum length null sequence of a p-level linear feedback shift register is discussed. The analysis presented here answers the following questions :

(i) When the null sequence generated by the p-level n stage linear shift register is pseudorandom ?

(ii) When the autocorrelation function of a p-nary m-sequence, as generated by the linear shift register, is zero ?

3.8.1 The necessary and sufficient condition for the null sequence of a linear p-nary n stage shift register to be pseudorandom.

Consider a p-nary m-sequence generated by an n stage p-level linear feedback shift register. Let the m-sequence be represented by C as :

$$C = (c_0, c_1, \ldots c_{N-1}),$$

$$= \{c_i\}$$

of period $N = p^n - 1$, having p^{n-1} digits for each of the $p - 1$ nonzero kinds, and $p^{n-1}-1$ zeros. Further, the second half of the sequence is the modulo-p complement of its first

half. Thus denoting $u = (N - 2)/2$,

$$C = (c_o, c_1, c_2, \ldots c_{N-1})$$

$$= (c_o, c_1, c_2, \ldots c_u, p-c_o, p-c_1, \ldots p-c_{N-1})$$

Also, let 's' represent any nonzero digit (1, 2, ...,p - 1) with a corresponding analogue level 'α_s'.

For any delay τ, the value of the autocorrelation function of the m-sequence C is given by :

$$\phi_{CC}(\tau) = \frac{1}{N} \sum_{i=1}^{N} c_i \, c_{i+\tau} \quad .. \quad 0 \leq \tau \leq N - 1 \quad .. \quad (3.39)$$

Owing to its antisymmetric nature, the autocorrelation function for $\frac{N+1}{2} \leq \tau \leq N - 1$ is the negative of that for $0 \leq \tau \leq \frac{N-1}{2}$, when analogue levels of the nonzero digits are adjusted for symmetry. It is, therefore, of interest to consider the value of the autocorrelation function in the range $0 \leq \tau \leq \frac{N-1}{2}$

The right hand side of eqn. (3.39) may be considered as the sum of another sequence $\{e_i\}$, which is formed by shifting the sequence $\{c_i\}$ relative to itself and forming the product of the corresponding digits. Hence,

$$e_i = c_i c_{i+\tau} \quad \ldots \quad \ldots \quad (3.40)$$

Since the terms of the sequence $\{c_i\}$ are integers in the modular field (0, 1, 2, ... p - 1), a term of the sequence $\{e_i\}$

must be formed by the product of any one of the following combinations :

(i) (0, 0)

(ii) (0, s)

(iii) (s, s)

(iv) (r, s) $\quad r \neq s$ and $r, s = (1, 2, \ldots p-1)$

We assume here that the order is unimportant and we need not distinguish between, say, (r, s) and (s, r).

Denote the number of occurrances of these combinations as :

$L_{oo}(\tau)$ = Number of (0, 0)

$L_{os}(\tau)$ = " (0, s)

$L_{ss}(\tau)$ = " (s, s)

$L_{rs}(\tau)$ = " (r, s)

These numbers determine the structure of the product sequence $\{e_i\}$.

Next, we obtain $L_{oo}(\tau)$, $L_{os}(\tau)$, $L_{ss}(\tau)$, $L_{rs}(\tau)$ in terms of the parameters of the sequence by means of deduction method as follows :

For this purpose, consider the following four cases :

(i) Modulus p = 3

Number of stages in the shift register, n = 2

characteristic equation of the fsr : $(2 + 2D + D^2)C = 0$

where Q is the basic m-sequence.

Basic m-sequence C is :

C : 1 2 2 0 2 1 1 0, ... with period $N = p^n - 1 = 8$ digits

For any delay τ in the range $0 < \tau \leq \frac{N-1}{2}$, for this m-sequence the following values of $L_{oo}(\tau)$, $L_{os}(\tau)$, $L_{ss}(\tau)$, $L_{rs}(\tau)$ are obtained - (r, s = 1, 2; $r \neq s$)

$L_{oo}(\tau) = 0$
$L_{os}(\tau) = 4$
$L_{ss}(\tau) = 2$
$L_{rs}(\tau) = 2$

For p = 3, n = 2

(ii) Modulus p = 3

Number of stages in the shift register, n = 3.

Characteristic equation of the fsr : $(2 + D^2 + 2D^3)C = 0$

where C is the basic m-sequence.

Basic m-sequence C is :

C : 0 1 2 1 1 2 0 1 1 1 0 0 2 0 2 1 2 2 1 0 2 2 2 0 0 1,...

with period $N = p^n - 1 = 26$ digits.

For any delay τ in the range $0 < \tau \leq \frac{N-1}{2}$, for this m-sequence, the following values for $L_{oo}(\tau)$, $L_{os}(\tau)$, $L_{ss}(\tau)$, $L_{rs}(\tau)$ are obtained - (r, s = 1, 2; $r \neq s$)

$L_{oo}(\tau) = 2$
$L_{os}(\tau) = 12$
$L_{ss}(\tau) = 6$
$L_{rs}(\tau) = 6$

For p = 3, n = 3

(iii) Modulus p = 5

Number of stages in the shift register, n = 2.
Characteristic equation of the fsr: $(4 + 2D + 2D^2)C = 0$
where C is the m-sequence.

C : 2 4 2 2 3 0 1 2 1 1 4 0 3 1 3 3 2 0 4 3 4 4 1 0, ...

with period $N = p^n - 1 = 24$ digits.

For any delay τ in the range $0 < \tau \leq \frac{N-1}{2}$, for this m-sequence, the following values for $L_{oo}(\tau)$, $L_{os}(\tau)$, $L_{ss}(\tau)$, $L_{rs}(\tau)$ are obtained - (r, s = 1, 2, 3, 4, $r \neq s$).

$L_{oo}(\tau) = 0$
$L_{os}(\tau) = 8$
$L_{ss}(\tau) = 4$
$L_{rs}(\tau) = 12$

For $p = 5$, $n = 2$

(iv) Modulus p = 5

Number of stages in the fsr, n = 3.
Characteristic equation of the fsr : $(4 + 3D + 2D^3)C = 0$
where C is the m-sequence.

C: 0 2 3 4 1 4 0 2 4 2 0 3 3 4 3 0 3 0 0 1 3 4 4 3 2 4 3 3 2 2 2
0 4 1 3 2 3 0 4 3 4 0 1 1 3 1 0 1 0 0 2 1 3 3 1 4 3 1 1 4 4 4
0 3 2 1 4 1 0 3 1 3 0 2 2 1 2 0 2 0 0 4 2 1 1 2 3 1 2 2 3 3 3
0 1 4 2 3 2 0 1 2 1 0 4 4 2 4 0 4 0 0 3 4 2 2 4 1 2 4 4 1 1 1,..

with period $N = p^n - 1 = 124$ digits.

For any delay τ in the range $0 < \tau \leq \frac{N-1}{2}$ for this m-sequence, the following values of $L_{oo}(\tau)$, $L_{os}(\tau)$, $L_{ss}(\tau)$, $L_{rs}(\tau)$ are obtained - ($r, s = 1, 2, 3, 4$, and $r \neq s$).

$$\left.\begin{aligned} L_{oo}(\tau) &= 4 \\ L_{os}(\tau) &= 40 \\ L_{ss}(\tau) &= 20 \\ L_{rs}(\tau) &= 60 \end{aligned}\right\} \quad \text{for } p = 5, \text{ and } n = 3$$

In view of the above mentioned results, (cases i,ii,iii, iv), in general, for any p-nary ($p > 2$ and prime) n-stage linear feedback shift register m-sequence of period $N = p^n - 1$ digits, the following equations are valid :

For $0 < \tau \leq \frac{N-1}{2}$ and $\frac{N}{2} < \tau < N$

$$\left.\begin{aligned} L_{oo}(\tau) &= p^{n-2} - 1 \\ L_{os}(\tau) &= 2\left[(p^{n-1} - 1) - (p^{n-2} - 1)\right] \\ L_{ss}(\tau) &= (p-1)\, p^{n-2} \\ L_{rs}(\tau) &= (p^n - 1) - L_{oo}(\tau) - L_{os}(\tau) - L_{ss}(\tau) \\ &= (p-1)(p-2)\, p^{n-2} \end{aligned}\right\} \quad (3.41)$$

Similarly, for $\tau = 0$, the following equations may be written;

$$\left.\begin{aligned} L_{oo}(\tau) &= p^{n-1} - 1 \\ L_{os}(\tau) &= L_{rs}(\tau) = 0 \\ L_{ss}(\tau) &= (p-1)(p^{n-1}) \end{aligned}\right\} \quad \ldots \quad (3.42)$$

For $\tau = \frac{N}{2}$, likewise, we may write the following equations :

$$\left.\begin{aligned} L_{oo}(\tau) &= p^{n-1} - 1 \\ L_{os}(\tau) &= L_{ss}(\tau) = 0 \\ L_{rs}(\tau) &= (p-1)(p^{n-1}) \end{aligned}\right\} \quad \ldots \qquad (3.43)$$

The results expressed in eqns. (3.41), (3.42), (3.43) show that $L_{oo}(\tau)$, $L_{os}(\tau)$, $L_{ss}(\tau)$, and $L_{rs}(\tau)$ are not only independent of τ over the chosen interval, but they are completely determined by p and n.

Making use of the above results, the autocorrelation function of the m-sequence C may be written as :

$$\begin{aligned} \phi_{cc}(\tau) &= \frac{1}{N} \sum_{i=0}^{N} c_i \, c_{i+\tau} \\ &= \frac{1}{N} \, p^{n-2}(\alpha_s^2 + \alpha_{rs}) \qquad , \quad r \neq s \qquad (3.44) \\ & \qquad\qquad\qquad\qquad\qquad\qquad r, s = 1, 2, \ldots, p-1. \end{aligned}$$

where α_r and α_s are the analogue levels of the states r and s in the m-sequence respectively.

Now,

$$\begin{aligned} \alpha_s^2 &= 1^2 + 2^2 + 3^2 + \ldots\ldots + (p-1)^2 \\ &= 2\left[1^2 + 2^2 + 3^2 + \ldots\ldots + \left(\frac{p-1}{2}\right)^2\right] \quad \text{(For a symmetric m-sequence signal)} \\ &= \frac{p(p-1)(p+1)}{12} \qquad \ldots \qquad \ldots \qquad (3.45) \end{aligned}$$

And

$$\alpha_{rs} = [(1)(2) + (1)(3) + \ldots + (1)(p-1) + (2)(1) + (2)(3) + \ldots + (2)(p-1) + (3)(1) + (3)(2) + \ldots + (3)(p-1) + \ldots\ldots\ldots\ldots\ldots + \ldots\ldots\ldots\ldots\ldots + (p-1)(1) + (p-1)(2) + \ldots + (p-1)(p-2)]$$

$$= [1 + 2 + 3 + \ldots + p-1]^2 - 1^2 + 2^2 + 3^2 + \ldots + (p-1)^2$$

For a symmetric m-sequence signal, the second half of the signal is the negative of the first half.

Hence,

$$\alpha_{rs} = 0 - 2\left[1^2 + 2^2 + \ldots + \left(\frac{p-1}{2}\right)^2\right]$$

$$= -\frac{p(p-1)(p+1)}{12} \quad \ldots \quad \ldots \quad (3.46)$$

Substituting the values of α_s^2 and α_{rs} in eqn. (3.44), we obtain -

$$\phi_{CC}(\tau) = 0 \qquad \text{For } 0 < \tau \leq \frac{N-1}{2}$$

$$\text{and for } \frac{N}{2} < \tau < N \quad \ldots \quad (3.47)$$

In view of eqns. (3.41), (3.42), (3.43) and (3.47), we may now state that invariance of $L_{oo}(\tau)$, $L_{os}(\tau)$, $L_{ss}(\tau)$ and $L_{rs}(\tau)$ with τ is the necessary and sufficient condition for a p-level linear shift register null sequence to be pseudorandom.

Also, from eqn. (3.47), the condition for a p-nary linear feedback shift register sequence of period N to have zero autocorrelation function for any nonzero τ (except for $\tau = N/2$) is :

$$\alpha_s^2 = -\alpha_{rs}$$

Thus, given a linear p-level shift register sequence, it is possible to ascertain as to whether it is pseudorandom or otherwise. Also, the condition for the sequence to possess zero autocorrelation for any nonzero τ (except for $\tau = N/2$) may be verified from eqns. (3.45) and (3.46).

3.9 GENERATION OF PSEUDORANDOM SIGNALS CORRESPONDING TO m-SEQUENCES OVER GF($p = 2^2$)

The fundamental properties of recurrent sequences and maximum length sequences over GF(p = 2) have been discussed in Chapter 1. In this chapter, so far, the theory of maximum length sequences over GF(p > 2and prime) has been developed; but few properties have been described in the literature concerning $p = 2^m$, m being an integer. (Balza et.al. 1970, Zierler 1959, Godfrey et. al. 1968, Power and Simpson 1970, Brown 1969, Simpson and Power 1970, these include application of 4-level or almost a periodic sequences in system identification).

In the present section, a simple method is presented for generating 4-level pseudorandom signals, derived from their corresponding m-sequences, using a single binary feedback shift

register unit. The method becomes more effective in saving components as the period of the m-sequence increases.

3.9.1 Delay polynomial generating 4-level m-sequence

It is well known that a maximum length sequence of period $p^n - 1$ digits is obtained from such a recurrent relation as - (' + ' stands for mod-p addition)

$$a_o c_k + a_1 c_{k+1} + a_2 c_{k+2} + \cdots + a_{n-1} c_{k+n-1} + a_n c_{k+n} = 0 \quad \ldots (3.48)$$

where a_i and c_i belong to a Galois field of p elements, and

$$(a_o + a_1 D + a_2 D^2 + \cdots + a_{n-1} D^{n-1} + a_n D^n)\, C = 0 \quad \ldots (3.49)$$

is the characteristic equation of the corresponding linear shift register. Here the symbol D^j is the algebraic delay operator, the effect of which is to delay by j digits the variable (m-sequence C) it operates on. The term within the brackets of eqn. (3.49) is known as the characteristic delay polynomial, which must be primitive to realize maximum length sequence.

For the case of p = 4, which is considered in this section, the elements of GF(p = 4) may be designated as (0, 1, a, b). The additional multiplication rules over GF(4) are stated in Table 3.6 . A list of primitive delay polynomials over GF(4) is given in Table 3.7 .

Table 3.6

Addition over GF(4)

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Multiplication over GF(4)

.	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Table 3.7 Primitive polynomials over GF(4)

Degree of polynomial n	Primitive polynomial F(D)	Period in digits
3	$a + D + D^2 + D^3$	63
3	$b + D + D^2 + D^3$	63
3	$a + bD + D^2 + D^3$	63
3	$b + aD + D^2 + D^3$	63
3	$a + D + bD^2 + D^3$	63
3	$b + D + aD^2 + D^3$	63
4	$a + aD + aD^2 + D^3 + D^4$	255
4	$b + bD + bD^2 + D^3 + D^4$	255
4	$b + bD + aD^2 + 0D^3 + D^4$	255
4	$a + aD + bD^2 + 0D^3 + D^4$	255
4	$a + bD + 0D^2 + aD^3 + D^4$	255
4	$b + aD + 0D^2 + bD^3 + D^4$	255
4	$a + bD + D^2 + 0D^3 + D^4$	255

(continued)

Degree of polynomial n	Primitive polynomial F(D)	Period in digits
4	$b + aD + \mathbb{R}^2 + oD^3 + D^4$	255
4	$a + aD + aD^2 + \emptyset D^3 + D^4$	255
4	$b + bD + bD^2 + 0D^3 + D^4$	255
4	$a + bD + bD^2 + 0D^3 + D^4$	255
4	$b + aD + aD^2 + 0D^3 + D^4$	255
4	$a + D + 0D^2 + D^3 + D^4$	255
4	$b + D + 0D^2 + D^3 + D^4$	255
4	$a + bD + D^2 + bD^3 + D^4$	255
4	$b + aD + D^2 + aD^3 + D^4$	255
5	$b + 0D + bD^2 + aD^3 + D^4 + D^5$	1023
5	$a + 0D + aD^2 + bD^3 + D^4 + D^5$	1023

3.9.2 Statement of the problem

Consider now a 2-stage 4-level shift register shown in Fig. (3.6). The characteristic equation of the shift register may be written as :

$$(a + D + D^2)C = 0 \quad \ldots \quad \ldots \quad (3.50)$$

The corresponding recurrence relation is given by :

$$c_k = b\, c_{k+1} + b\, c_{k+2} \quad \ldots \quad \ldots \quad (3.51)$$

Assuming the initial state, 'c_{k+1}, c_{k+2}' of the shift register as ' a b ' , the succession of states in the register are as follows :

Table 3.8

Description of sequence	State numbers														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Output of stage 1	a	b	b	0	a	1	a	a	0	1	b	1	1	0	b,..
Output of stage 2	b	a	b	b	0	a	1	a	a	0	1	b	1	1	0,..
Ihput to stage 1	b	b	0	a	1	a	a	0	1	b	1	1	0	b	a,..

Let C represent the basic 4-level m-sequence of the 2-stage shift register (i.e. input to stage 1). Let x(t) be the signal corresponding to the m-sequence C. The present problem is to realize the signal x(t) by means of a binary shift register.

1.9.3 Generation of 4-level m-sequence signal using binary logic

Let the GF(4) elements 0, 1, a, b correspond with the analogue levels as under :

GF(4) elements	Corresponding analogue level
0	-1.5
1	-0.5
a	+0.5
b	+1.5

The selected analogue levels are symmetrical about zero. Under the circumstances, the 4-level signal x(t) may be thought of as an analogue sum of three binary component signals, say, $x_1(t)$, $x_2(t)$ and $x_3(t)$ as shown below :

Let us suppose that the states 1 and 0 in the component binary signals $x_1(t)$, $x_2(t)$, and $x_3(t)$ are maintained at analogue levels +0.5 and -0.5 respectively, i.e.

GF(2) elements	Corresponding analogue level
1	+ 0.5
0	- 0.5

Here, it is important to bear in mind that these binary levels (+0.5 and -0.5) of the component signals $x_1(t)$, $x_2(t)$ and $x_3(t)$ are different from the levels of the quarternary (i.e 4-level) m-sequence signal x(t), namely (-1.5, -0.5, +0.5, +1.5).

Under the circumstances, the GF(4) elements 0, 1, a, b may be expressed in terms of GF(2) elements, 0 and 1 as under :

GF(4) elements		GF(2) elements	
0	=	Analogue sum :	(0 + 0 + 0)
1	=	Analogue sum :	(0 + 0 + 1)
a	=	Analogue sum :	(1 + 1 + 0)
b	=	Analogue sum :	(1 + 1 + 1)

Making use of the correspondence between GF(4) elements and GF(2) elements mentioned above, the 4-level m-sequence signal x(t) is written below as an analogue sum of these component binary signals $x_1(t)$, $x_2(t)$ and $x_3(t)$:

Component binary signal	Succession of states in the binary signal															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15,	..
$x_1(t)$	1	1	0	1	0	1	1	0	0	1	0	0	0	1	1,	...
$x_2(t)$	1	1	0	1	0	1	1	0	0	1	0	0	0	1	1,	...
$x_3(t)$	1	1	0	0	1	0	0	0	1	1	1	1	0	1	0,	...
$x(t)=\sum_{i=1}^{3} x_i(t)$	b	b	0	a	1	a	a	0	1	b	1	1	0	b	a,	...

Therefore, the problem of generating the 4-level signal x(t) settles down to that of generating the above specified component signals. A close look at the content of the above table reveals that the signals $x_1(t)$ and $x_2(t)$ are identical and the signal $x_3(t)$ is merely the signal $x_1(t)$ delayed by ten digits. Thus, the formulation of 4-level m-sequence signal settles down to the problem of generating the signal $x_1(t)$.

Generation of the binary signal $x_1(t)$:

The sequence x_1 corresponding to the signal $x_1(t)$ is of period equal to 15 bits. Further,† it describes $2^4 - 1$ nonzero states of a 4-stage mod-2 feedback binary shift register. Hence, it is possible to generate the signal $x_1(t)$ with the help of a binary shift register with suitable mod-2 feedback.

In Chapter 1 (Section 1.7.2) it has been shown that it is possible to find the logical configuration of the shift register

† Provided the characteristic polynomial of the 4-level shift-register under consideration is primitive over GF(4), the sequence x_1 so obtained, describes 2^n-1 (n = integer) distinct binary numbers.

that generates a given binary sequence by means of the generating function concept.

Assuming the initial state of the binary shift register as ' 0 0 ... 1 ', it has been shown that the generating function associated with the sequence x_1 is related to the delay polynomial of the corresponding shift register by the following equation (Eqn. 1.15 repeated below) -

$$G(x) = \frac{I}{F(D)\,x}$$

where G(x) and F(D), respectively, represent the generating function and the delay polynomial of the sequence under consideration.

Since the sequence is periodic, we need to consider only one period of the sequence, and write the generating function associated with the sequence of present interest, namely, x_1 as -

$$G_1(x_1) = (I + D + D^2 + D^3 + D^5 + D^7 + D^8 + D^{11})$$ (mod-2 addition)

With the help of eqn.(1.15) written above, the delay polynomial F(D) of the sequence x_1 (i.e. the feedback connections of the binary shift register generating the sequence x_1) is :

$$[F(D)]\, x_1 = \frac{I}{G_1(x_1)} = (I + D + D^4)\, x_1$$ ..(mod-2 addition)

Thus, the component sequence x_1 may be generated directly by means of a 4-stage binary feedback shift register, wherein the modulo-2 sum of the contents of first stage and fourth stage provides input to the first stage. The table below shows the succession of states in this binary shift register.

Table 3.9

Description of sequence	State number in the binary shift register														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15,...
Output of stage 1	1	0	1	1	0	0	1	0	0	0	1	1	1	1	0 ,...
Output of stage 2	0	1	0	1	1	0	0	1	0	0	0	1	1	1	1,...
Output of stage 3	1	0	1	0	1	1	0	0	1	0	0	0	1	1	1,...
Output of stage 4	1	1	0	1	0	1	1	0	0	1	0	0	0	1	1,...
Input to stage 1	0	1	1	0	0	1	0	0	0	1	1	1	1	0	1,...

From the content of the above table, it is clear that the sequence x_1 (with the chosen initial state of the binary shift register) is available at the output of stage 4. The sequence x_2 corresponding to the component signal $x_2(t)$ is the same as the

sequence x_1. Further the sequence x_3 corresponding to the component signal $x_3(t)$ is the sequence x_1 delayed by ten bits. Hence, it may be obtained by modulo-2 sum of shift, third and fourth stage outputs as shown below -

$$x_3 = D^{10} x_1$$

$$= D^{10}(D^4 x_1^*), \qquad x_1^* \text{ represents input to stage 1 (Fig. 3.7)}$$

$$= (D + D^3 + D^4)\, x_1^*$$

To realise the signals corresponding to the component sequences x_1, x_2, x_3 we need to transform the states 1 and 0 to the levels +0.5 and -0.5 respectively. And the analogue sum of the so obtained signals $x_1(t)$, $x_2(t)$ and $x_3(t)$ provides the desired 4-level m-sequence signal x(t). Fig. (3.7a) details the practical scheme of generating the said multilevel signal x(t). The so generated 4-level m-sequence signal together with component signals is shown in Fig. (3.8a,b) (Photographs).

Thus it is possible to generate 4-level pseudorandom signals, derived from their corresponding m-sequences, using a single binary feedback shift register unit. The method becomes more effective in saving components as the period of m-sequence increases. In general, pseudorandom signals over GF($p = 2^m$, m an integer) can be easily generated using this technique.

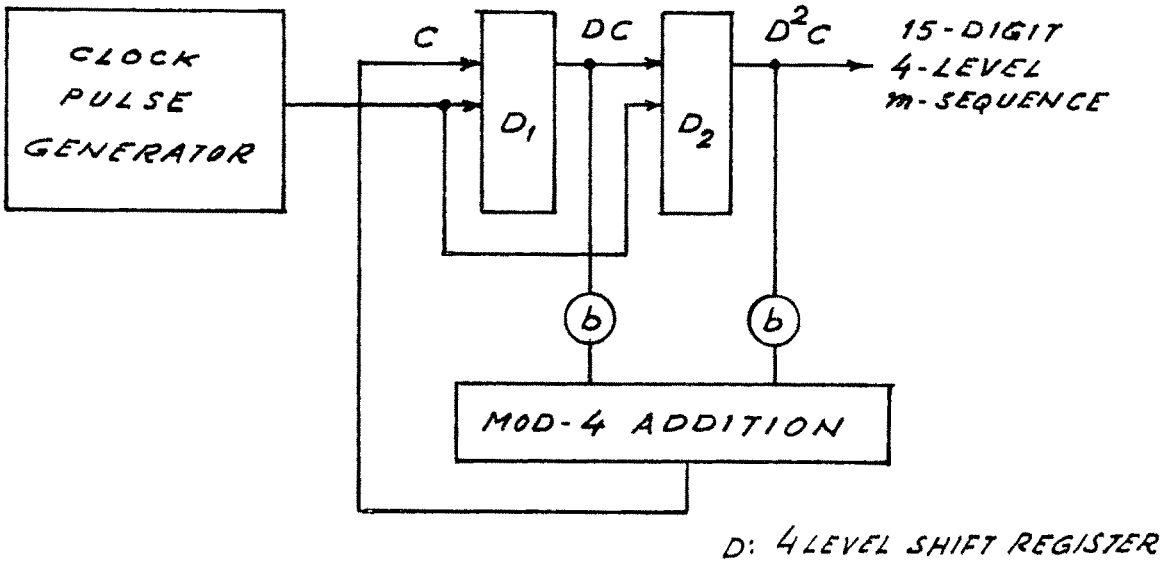


FIG. 3·6 2 STAGE 4-LEVEL FEEDBACK SHIFT REGISTER

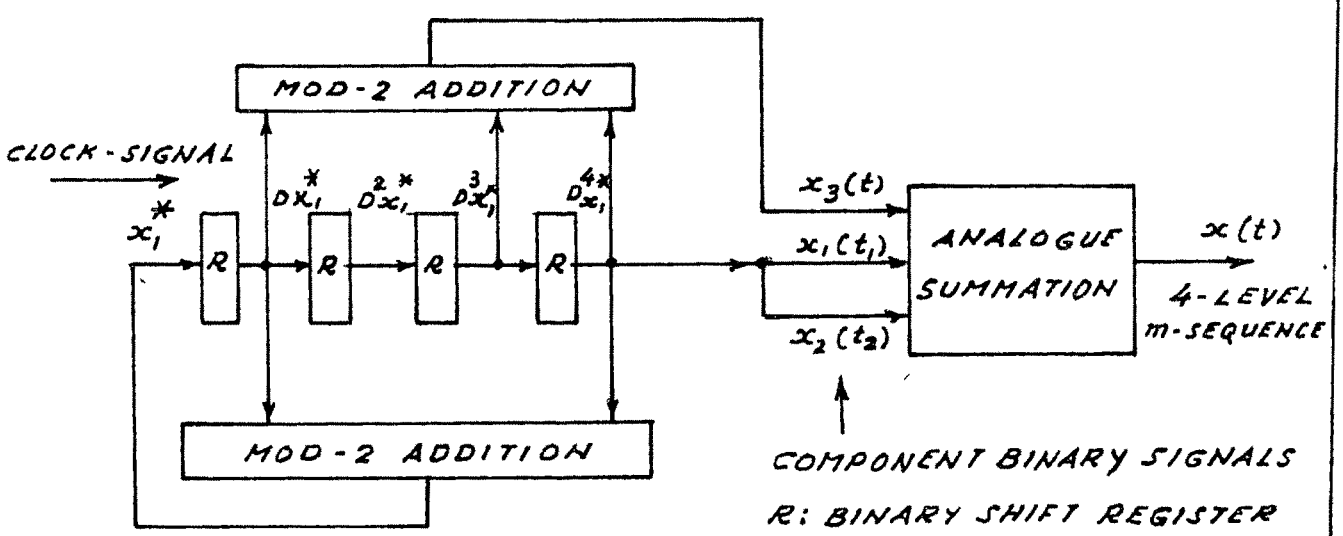


FIG. 3·7 PRACTICAL SCHEME OF GENERATING 4-LEVEL m-SEQUENCE USING BINARY LOGIC-ELEMENTS

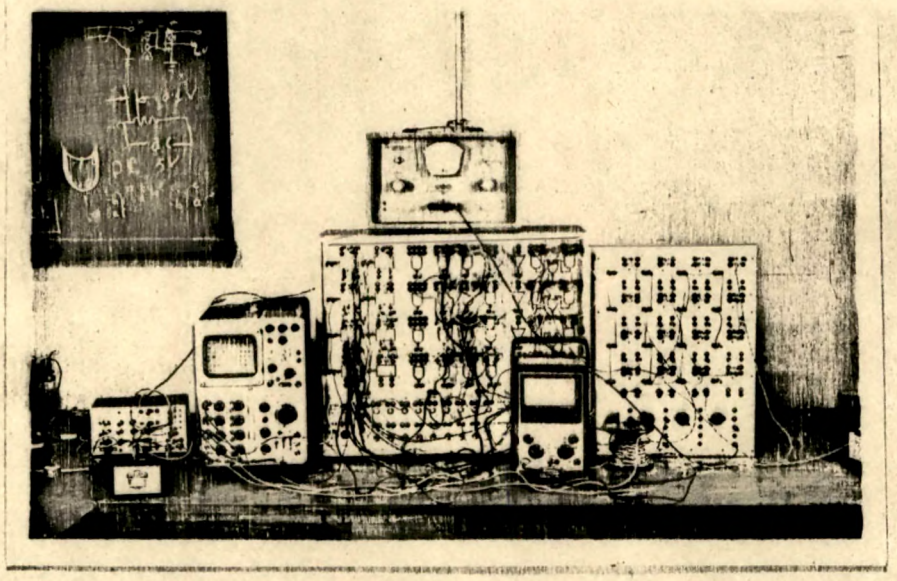


Fig.3.8 : Experimental set up for the generation of 15-bit 4-level m-sequence signal

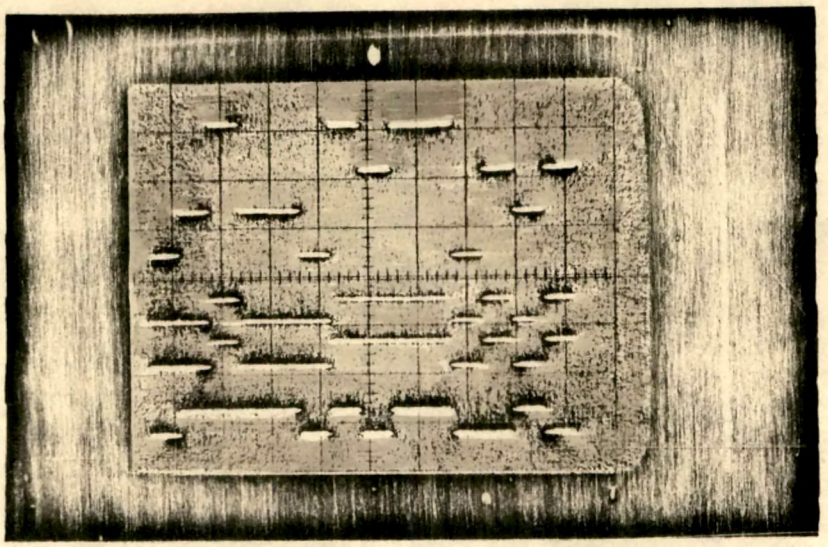


Fig.3.9 : (a) 15-bit 4-level m-sequence signal $x(t)=\sum_{i=1}^{3} x_i(t)$

(b) Component binary signal $x_1(t)$

(c) Component binary signal $x_2(t) = x_1(t)$

(d) Component binary signal $x_3(t)$

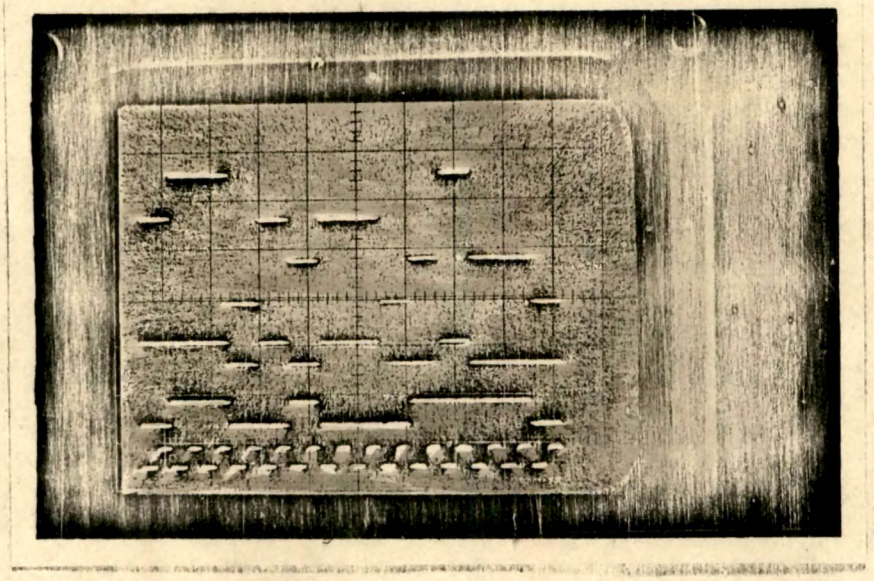


Fig.3.10: (a) 15-bit 4-level m-sequence signal x(t)
(b) Component binary signal $x_1(t) = x_2(t)$
(c) Component binary signal $x_3(t)$
(d) Clock signal

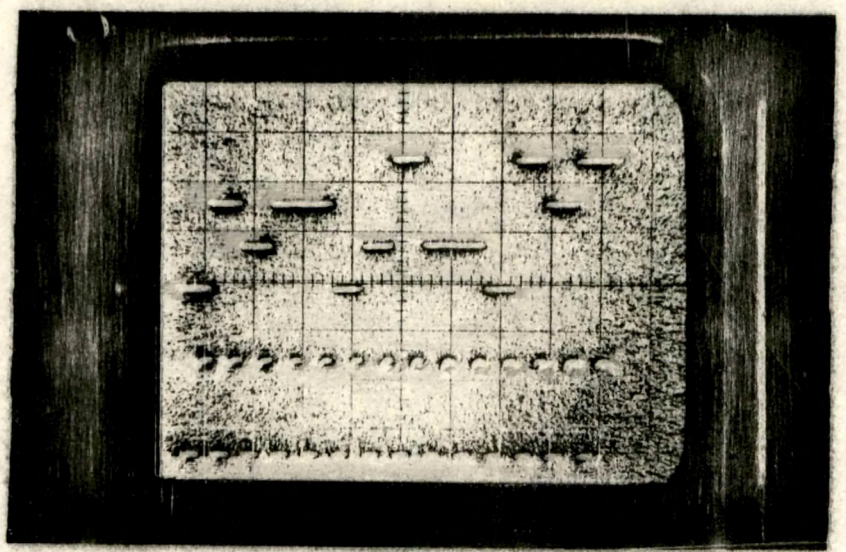


Fig.3.11: (a) 4-level m-sequence signal x(t)
(b) Clock signal

3.10 SUMMARY

In this chapter, the theory of multilevel linear feedback shift register sequences has been developed in some depth. Methods are presented to derive the sequential behaviour analytically from the knowledge of the given multilevel shift register logical structure. Attention is also given to the synthesis problem of realizing a given cycle structure. Furthermore, a quick method of finding the multistable feedback shift register connections for providing delayed replicas of the basic m-sequence is advanced, making use of generating function concept. A few of the most important properties of the multilevel sequences are discussed. Also, a structural property of linear p-nary shift register sequences is broughtforth, which is useful in determining as to whether a given p-nary sequence is pseudorandom or otherwise. And, an attempt is made to describe generation of pseudorandom signals corresponding to m-sequences over GF($p = 2^2$) with the help of binary logic elements, which is successfully experimented.

In the following chapter, the problem of multi-input / multi - output system identification with pseudorandom test signals (binary as well as multilevel m-sequence signals) by means of correlation method will be discussed.
