NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Technical Report 32-1432

Pseudonoise Sequence Generation With Three-Tap Linear Feedback Shift Registers

Marvin Perlman

JET PROPULSION LABORATORY
CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA

November 15, 1969

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Technical Report 32-1432

Pseudonoise Sequence Generation With Three-Tap Linear Feedback Shift Registers

Marvin Perlman

JET PROPULSION LABORATORY
CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA

November 15, 1969

Prepared Under Contract No. NAS 7-100
National Aeronautics and Space Administration

Preface

The work described in this report was performed by the Space Sciences Division of the Jet Propulsion Laboratory.

Contents

Tables

Figure

Abstract

Linear recurring binary sequences with pseudonoise properties may be generated by shift registers with linear (logic) feedback. An r-stage linear FSR is characterized by an rth degree polynomial in one indeterminant, with coefficients taken from a field of two elements. The two-tap r-stage linear FSR characterized by an rth-degree primitive trinomial over $GF(2)$ is the most efficient generator in terms of implementation of a PN sequence. Primitive trinomials do not exist, however, for every value of r.

This paper deals with a search for rth-degree tetranomials through degree 34 which contain either an $r-1$th-degree or an $r-2$th-degree primitive polynomial over $GF(2)$ as a factor. The tetranomials characterize a three-tap r-stage linear FSR capable of generating PN sequences of length $2^{r-1}-1$ or $2^{r-2}-1$ when properly initialized.

A *primitive trinomial does not exist* of degree $r-1$ equal to 8, 12, 13, 14,16, 19, 24, 26, 27, 30, and 32. *Tetranomials* of degree r *do exist*, however, which contain as a factor a *primitive polynomial* of degree $r-1$ for each of the preceding values of $r-1$ except 12.

Pseudonoise Sequence Generation With Three-Tap Linear Feedback Shift Registers

I. Introduction

A. Irreducible Polynomials over GF(p) and Finite Fields

The integers, $0, 1, \cdots, p-1$, where p is prime, form a field under the binary operations of addition and multiplication modulo p. The field is termed a *Galois field of p elements* (Ref. 1) and is denoted as $GF(p)$.

Consider polynomials in one indeterminant whose coefficients are taken from the field $GF(p)$. Such a polynomial $f(x)$ of degree $m \geq 1$ is irreducible over $GF(p)$ if it cannot be expressed $f(x) = g(x)\ h(x)$, where $g(x)$ and $h(x)$ are polynomials over $GF(p)$ of degree less than m. The set of polynomials

$$a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} \tag{1}$$

where $a_i \in GF(p)$ form a field. The binary operations are addition (of two polynomials) modulo $f(x)$ and multiplication (of two polynomials) modulo $f(x)$, where $f(x)$ is irreducible over $GF(p)$ and of degree m. This is termed a *Galois field of p^m elements* and is denoted as $GF(p^m)$. An irreducible polynomial over $GF(p)$ plays a role analogous to that of the integer p in forming a field. Every abstract finite field is of order p^m, where $m \geq 1$ and is isomorphic to a $GF(p^m)$.

The nonzero elements of $GF(p)$ form a cyclic multiplicative group of order $p-1$. Furthermore,

$$a^{p-1} \equiv 1 \bmod p \tag{2}$$

for any integer $a \not\equiv 0 \bmod p$. Thus (2) holds for every nonzero element of $GF(p)$. This is a well-known theorem of Fermat (Ref. 2). The multiplicative order of each nonzero $a_i \in GF(p)$ is the least integer n for which

$$a_i^n \equiv 1 \bmod p \tag{3}$$

The order of a_i divides the order of the multiplicative group. That is, n divides $p-1$. This is a consequence of Lagrange's theorem (Ref. 1), which states the order of a subgroup divides the order of the group. An element a_i with order $n = p-1$ is defined as a *primitive element* of $GF(p)$. Every $GF(p)$ contains $\varphi(p-1)$ primitive elements, each of which is a *generator* of the cyclic multiplicative group. The Euler phi-function $\varphi(n)$ (Ref. 2) is the number of integers no greater than the integer n that are relatively prime to n. The evaluation of $\varphi(n)$ is as follows:

$$\varphi(n) = \begin{cases} 1 \text{ for } n = 1 \\ p-1 \text{ for } n = p \text{ a prime} \\ \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1) \text{ for } n = \prod_{i=1}^{k} p_i^{e_i} \end{cases}$$

An irreducible polynomial $f(x)$ over $GF(p)$ has α as a root such that $f(\alpha) = 0$. If $f(x)$ is of degree m, α^m may be expressed as

$$\alpha^m = -\sum_{i=0}^{m-1} a_i \alpha_i \tag{4}$$

Furthermore, the elements of the field (1) may be expressed as

$$a_0 + a_1 \alpha^1 + \cdots + a_{m-1} \alpha^{m-1} \tag{5}$$

The field $GF(p)$ is termed the *ground field* and $GF(p^m)$ as shown in (5) is known as the *extension field* of degree m over $GF(p)$.

The nonzero elements of $GF(p^m)$ form a cyclic multiplicative group of order p^m-1. Also as in (2),

$$[y_i(\alpha)]^{p^m-1} \equiv 1 \bmod f(\alpha) \tag{6}$$

for any nonzero element $y_i(\alpha)$ of the extension field $GF(p^m)$. The multiplicative order of each nonzero element of $GF(p^m)$ divides $p^m - 1$. An element $y_i(\alpha)$ with order $n = p^m-1$ is defined as a *primitive element* of the *extension field* $GF(p^m)$. Every extension field $GF(p^m)$ contains $\varphi(p^m - 1)$ primitive elements, each of which is a *generator* of the cyclic multiplicative group.

If α is a root of an mth degree irreducible polynomial $f(x)$ over $GF(p)$, then α^p, α^{p^2}, $\cdots$, $\alpha^{p^{m-1}}$ are also roots of $f(x)$. Furthermore, all the roots have the same multiplicative order. The *period* of an irreducible polynomial $f(x)$ over $GF(p)$ is defined as the order of its roots. Equivalently, the period of $f(x)$ is the least integer n for which $f(x)$ divides x^n-1. Note that α is a root of x^n-1 since

$$\alpha^n \equiv 1 \bmod f(\alpha) \tag{7}$$

where n is the order of α. Thus $f(x)$ must be a factor of x^n-1.

Whenever a root of $f(x)$ is a primitive element of the extension field $GF(p^m)$, $f(x)$ is defined as a *primitive polynomial* over $GF(p)$ and has a period of $n = p^m-1$.

The period of any polynomial $g(x)$ over $GF(p)$ is the least integer n for which $g(x)$ divides $x^n - 1$. If $g(x)$ is irreducible but not primitive, n is less than $p^m - 1$ and n divides p^m-1. If $g(x)$ is primitive, n equals p^m-1. When $g(x)$ is reducible, n is a number-theoretic function of the periods of its irreducible factors over $GF(p)$ (see Section I-B).

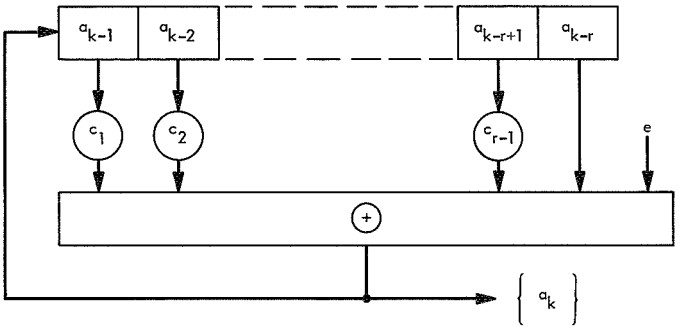

Fig. 1. An *r*-stage linear feedback shift register

B. Linear Feedback Shift Registers and Polynomials over GF(2)

The (binary) linear logic feedback shift register (FSR) shown in Fig. 1 has been investigated in considerable detail (Ref. 3). The state of the ith two-state memory element at clock pulse interval (CPI) k is denoted as a_{k-i}. The behavior of the FSR can be characterized by the linear recurrence relationship.

$$a_k = e + \sum_{i=1}^{r} c_i \, a_{k-i} \tag{8}$$

The bit fed back at CPI k is denoted as a_k. The ith stage contributes to the feedback when the Boolean multiplier c_i is at state-value 1. The summations are taken modulo 2, and e, a Boolean constant, is 0 for mod 2 summing (EXCLUSIVE-OR) or 1 for the complement of mod 2 summing (NOT EXCLUSIVE-OR).

The cycle length or periodicity of $\{a_k\}$ for a given initial state can be determined from its generating function (Ref. 3)

$$G_e^r(x) = \sum_{k=0}^{r} a_k x^k = \sum_{k=0}^{\infty} \left(e + \sum_{i=1}^{r} c_i \, a_{k-i} \right) x^k$$

For $e = 0$,

$$G_0^r(x) = \frac{\sum_{i=1}^{r} c_i x^i \left(a_{-i} x^{-i} + a_{-i+1} x^{-i+1} + \cdots + a_{-1} x^{-1} \right)}{1 + \sum_{i=1}^{r} c_i x^i} \tag{9}$$

where a_{-i} is the initial state of the ith stage. For $e = 1$,

$$G_1^r(x) = \sum_{k=0}^{\infty}\left(1 + \sum_{i=1}^{r} c_i\, a_{k-i}\right)$$

$$= \frac{1}{1+x} + \sum_{i=1}^{r} c_i\, x^i \sum_{k=0}^{\infty} a_{k-i}\, x^{k-i}$$

$$= \frac{1}{1+x} + \sum_{i=1}^{r} [c_i\, x^i\, a_{-i}\, x^{-i} + a_{-i+1}\, x^{-i+1} + \cdots + a_{-1}\, x^{-1} + G_1^r(x)]$$

$$G_1^r(x) = \frac{1 + (1+x)\sum_{i=1}^{r} c_i\, x^i\, (a_{-i}\, x^{-i} + a_{-i+1}\, x^{-i+1} + \cdots + a_{-1}\, x^{-1})}{(1+x)\left(1 + \sum_{i=1}^{r} c_i\, x^i\right)} \tag{10}$$

The generating functions $G_0^r(x)$ and $G_1^r(x)$ are the ratios of two polynomials over $GF(2)$ and may be expressed as

$$G_0^r = \frac{g_0(x)}{f_0(x)}$$

$$G_1^r = \frac{1 + (1+x)\, g_0(x)}{(1+x)\, f_0(x)} = \frac{g_1(x)}{f_1(x)}$$

The characteristic polynomial $f_e(x)$ is a function of the feedback connections only. The length of longest FSR cycle(s) is the least integer n for which $f_e(x)$ divides $x^n + 1$. (Note that $-1 \equiv 1 \bmod 2$.) This is precisely the period of $f_e(x)$.

The polynomial $g_e(x)$ is a function of the initial state of the register and the feedback connections. The degree of $g_e(x)$ is always less than that of $f_e(x)$. An initial state $a_{-1}\, a_2 \cdots a_{-r}$ which results in a $g_e(x)$ that is relatively prime to $f_e(x)$ will lie on a cycle whose length is n the period of $f_e(x)$. An initial state that yields a $g_e(x)$ that has a common factor with $f_e(x)$ will lie on a cycle whose length divides n. Thus all cycle lengths of an FSR with a characteristic polynomial $f_e(x)$ divide n the period of $f_e(x)$.

The initial state $00 \cdots 01$ results in $g_0(x) = 1$, and

$$G_0^r(x) = \frac{1}{1 + \sum_{i=1}^{r} c_i\, x^i} = \frac{1}{f_0(x)}$$

The initial state $00 \cdots 0$ results in $g_1(x) = 1$, and

$$G_1^r(x) = \frac{1}{(1+x)\left[1 + \sum_{i=1}^{r} c_i\, x^i\right]} = \frac{1}{f_1(x)}$$

Each of these initial states lies on a cycle of longest possible length.

Example 1. Consider $a_k = a_{k-1} + a_{k-2} + a_{k-4}$. The initial state $a_{-1}\, a_{-2}\, a_{-3}\, a_{-4}$ of 0001 lies on a cycle of longest length represented by

$$G_0^4(x) = \frac{1}{1 + x + x^2 + x^4} = \frac{1}{f_0(x)}$$

$$= 1 + x + x^3 + x^7 + x^8 + x^{10} + \cdots$$

The coefficients of x correspond to the bits in the recurring sequence $\{a_k\}$ whose period is 7:

k	0	1	2	3	4	5	6
a_k	1	1	0	1	0	0	0

The 16 states of the four-stage FSR lie on four disjoint cycles. They are tabulated as follows, with a_{k-i} denoted as a_i:

k	a_1	a_2	a_3	a_4	a_k	a_1	a_2	a_3	a_4	a_k
0	0	0	0	1	1	1	1	1	0	0
1	1	0	0	0	1	0	1	1	1	0
2	1	1	0	0	0	0	0	1	1	1
3	0	1	1	0	1	1	0	0	1	0
4	1	0	1	1	0	0	1	0	0	1
5	0	1	0	1	0	1	0	1	0	1
6	0	0	1	0	0	1	1	0	1	1
0	0	0	0	0	0	1	1	1	1	1

The four disjoint cycles correspond to the four recurring sequences (1101000), (0010111), (0), and (1), with periods 7, 7, 1, and 1, respectively. The period of the longest cycle(s) corresponds to the period of $f_0(x)$.

The period of a polynomial can be determined from the period of its irreducible factors. The period of a repeated irreducible factor is determined as follows: If $\phi(x)$ is irreducible over $GF(2)$ and has period n, then $\phi(x) \mid x^n + 1$

Also,

$$(x^n + 1)^2 = x^{2n} + 1$$

and, by induction,

$$(x^n + 1)^{2^i} = x^{2^i n} + 1$$

Therefore,

$$[\phi(x)]^s \mid (x^n + 1)^{2^i} = x^{2^i n} + 1$$

where $2^{i-1} < s \leq 2^i$, and the period of $[\phi(x)]^s$ is $2^i n$.

The period of

$$g(x) = [\phi_1(x)]^{s_1} [\phi_2(x)]^{s_2} \cdots [\phi_t(x)]^{s_t}$$

is

$$\text{LCM}\left(2^{i_1} n_1, 2^{i_2} n_2, \cdots, 2^{i_t} n_t\right)$$

where LCM denotes the least common multiple.

In example 1,

$$f_0(x) = (1 + x)(1 + x^2 + x^3)$$

The periods of the irreducible factors are 1 and 7. The period of $f_0(x)$ is LCM (1, 7) or 7.

Example 2. Consider $a_k = 1 + a_{k-1} + a_{k-2} + a_{k-4}$. The initial state $a_{-1}\, a_{-2}\, a_{-3}\, a_{-4}$ of 0000 lies on a cycle of longest length represented by

$$G_1^4(x) = \frac{1}{(1 + x)(1 + x + x^2 + x^4)}$$

$$= \frac{1}{(1 + x)^2 (1 + x^2 + x^3)} = \frac{1}{f_1(x)}$$

The period of $f_1(x)$ is LCM $[2 \cdot 1, 7]$ or 14. The 16 states of the four-stage FSR lie on two disjoint cycles:

k	a_1	a_2	a_3	a_4	a_k
0	0	0	0	0	1
1	1	0	0	0	0
2	0	1	0	0	0
3	0	0	1	0	1
4	1	0	0	1	1
5	1	1	0	0	1
6	1	1	1	0	1
7	1	1	1	1	0
8	0	1	1	1	1
9	1	0	1	1	1
10	1	1	0	1	0
11	0	1	1	0	0
12	0	0	1	1	0
13	0	0	0	1	0
0	0	1	0	1	1
1	1	0	1	0	0

The two disjoint cycles correspond to the recurring sequences (10011110110000) and (10).

The numerator of $G_1^4(x)$ in example 2 for an arbitrary initial state $a_{-1}\, a_{-2}\, a_{-3}\, a_{-4}$ is $g_1(x) = (1 + a_{-1} + a_{-2} + a_{-4}) + (a_{-2} + a_{-3} + a_{-4})\, x + (a_{-1} + a_{-2} + a_{-3})\, x^2 + (a_{-1} + a_{-2})\, x^3 + a_{-1}\, x^4$. For the initial state 0101,

$$g_1(x) = 1 + x^2 + x^3$$

and

$$G_1^4(x) = \frac{g_1(x)}{f_1(x)} = \frac{1}{(1 + x)^2} = \frac{1}{1 + x^2}$$

which corresponds to the recurring sequence (10).

C. Tables of Irreducible Polynomials over GF(2)

In 1953 Gilbert (Ref. 4) determined values of a and b which guaranteed the primitiveness or the imprimitiveness of trinomials $1 + x^a + x^b$ through degree $b = 31$. There were many values of a and b for which primitiveness was not proved or disproved. Marsh's tables (Ref. 5) contain all the irreducible polynomials over $GF(2)$ and their respective periods through degree 19. Golomb, Welch, and Hales generated two tables of trinomials over $GF(2)$. One table contains the irreducible factors of each trinomial of degree ≤ 36 together with the period

of each trinomial and of each irreducible factor. The second table contains the factor of lowest degree for trinomials of degree 37 through 45. These tables appear in Ref. 3. Peterson's tables (Ref. 6) contain information about every irreducible polynomial over $GF(2)$ of degree ≤ 16. A primitive polynomial with a minimum number of terms and an irreducible polynomial corresponding to each possible period is given for every degree from 17 through 34. Watson (Ref. 7) lists one primitive polynomial over $GF(2)$ for every degree from 1 through 100. Zierler and Brillhart (Ref. 8) have generated two tables. One table contains a complete list of every irreducible trinomial over $GF(2)$ for every degree from 2 through 1000. The known primitive entries are noted. The second table contains the periods of some of the imprimitive polynomials.

Consider the sequence $\{a_k\}$ of period 2^r-1 generated by an r-stage FSR having a primitive rth-degree characteristic polynomial. This is a maximal-length FSR sequence which has three properties of randomness (Ref. 3). It is, therefore, frequently termed a pseudonoise or PN sequence. Applications of PN sequences include ranging, error detection and error correction coding, prescribed sequence generation, counting, scaling, and secure communications. The primitive trinomial characterizes the FSR of least complexity in terms of feedback combinational logic capable of generating a PN sequence.

The number of primitive polynomials of degree r is known to be (Ref. 3)

$$\lambda_2(r) = \frac{\varphi(2^r - 1)}{r} \tag{11}$$

The primitive polynomials are a subset of the irreducible polynomials. For degree r, the number of irreducible polynomials is:

$$\psi_2(r) = \frac{1}{r} \sum_{d|r} \mu(d)\, 2^{r/d} \tag{12}$$

where the sum is extended over all divisors d of r. The Möbius number-theoretic function $\mu(d)$ (Ref. 2) is defined as follows:

$$\mu(d) = \begin{cases} 1 \text{ for } d = 1 \\ 0 \text{ when } a^2 | d \text{ and } a > 1 \\ (-1)^k \text{ for } d = p_1 p_2 \cdots p_k \end{cases}$$

Note that $\lambda_2(r)$ and $\psi_2(r)$ are equal in the case when 2^r-1 is prime. (These are known as Mersenne primes; to date, the first 23 have been determined.)

Because of the large magnitudes of $\lambda_2(r)$ and $\psi_2(r)$ for even modest values of r, the search for irreducible polynomials of high degree has been restricted to trinomials.

Unfortunately, there are many values of r for which an irreducible trinomial of degree r does not exist. Furthermore, there are values of r for which irreducible but not primitive trinomials of degree r exist (Refs. 3, 8, 9).

II. Tetranomials over GF(2) of Degree r with Periods of $2^{r-1}-1$ or $2^{r-1}-2$

A. Search Technique

A 34-stage FSR was constructed to operate at a clock frequency of 1 MHz. Provisions were made to alter its length, insert any predetermined initial state, and feed back the modulo 2 sum (EXCLUSIVE-OR) or the complement of the modulo 2 sum (NOT EXCLUSIVE-OR) of the content of the stages i, j, and r, where r denotes the last stage and $i < j < r$. A word detector (effectively an r-input gate) was used to sense and "remember" the initial state. By means of control logic, the initial state is inserted, the word detector primed, the clock initiated, and the clock terminated when the FSR is returned to its initial state. The foregoing sequence of events yields a count of the number of clock pulses required for an FSR to return to an initial state. The count is equivalent to the length of the cycle containing the initial state.

B. Theorems

The linear recurrence relationships (i.e., feedback functions) of interest are of the following form:

$$a_k = a_{k-i} + a_{k-j} + a_{k-r} \tag{13}$$

The characteristic polynomial associated with (13) is

$$f_0(x) = 1 + x^i + x^j + x^r$$

A number of theorems are useful in verifying results and reducing the number of cases to be searched.

THEOREM 1 (REF. 3). *Every state of the FSR will have a unique predecessor and a unique successor (i.e., the cycles will be branchless) if and only if the feedback function can be decomposed as follows:*

$$a_k = F(a_{k-1}, a_{k-2}, \cdots, a_{k-r+1}) + a_{k-r}$$

where $F(a_{k-1}, a_{k-2}, \cdots, a_{k-r+1})$ is any Boolean function of the content of all stages but r. All linear feedback functions are of this form (8).

THEOREM 2 (REF. 3). *The number of cycles for $r > 2$ into which the 2^r states of an r-stage FSR is decomposed is even or odd according to whether the number of 1s in the truth table of $F(a_{k-1}, a_{k-2}, \cdots, a_{k-r+1})$ is even or odd.* When the feedback function is linear (8), the number of cycles is even.

THEOREM 3 (REF. 10). *The number of recurring sequences of length n is*

$$S(n) = \frac{1}{n} \sum_{d|n} \mu(d)\, 2^{n/d}$$

The sequences with periods $n = 1, 2, 3$, and 4 are tabulated as follows:

n	$S(n)$	Sequences
1	2	(0) (1)
2	1	(01)
3	2	(001) (011)
4	3	(0001) (0011) (0111)

THEOREM 4. (REF. 3). *If $F(a_{k-1}, a_{k-2}, \cdots, a_{k-r+1}) = F(a'_{k-1}, a'_{k-2}, \cdots, a'_{k-r+1})$, states $a_{k-1}\, a_{k-2}, \cdots, a_{k-r}$ and $a'_{k-1}\, a'_{k-2}, \cdots, a'_{k-r}$ will lie on cycles of the same length, which are complementary images of one another, or they will lie on the same cycle separated by 180 deg.*

THEOREM 5. *A necessary but not sufficient condition for a tetranomial $1 + x^i + x^j + x^r$ to have a period $2^{r-1}-1$ is that*

$$i + j + r \equiv 1 \bmod 2 \tag{14}$$

Proof. If $f_0(x) = 1 + x^i + x^j + x^r$ has period $2^{r-1}-1$, then

$$f_0(x) = (1 + x)\, \phi(x) \tag{15}$$

where $\phi(x)$ is a primitive polynomial of degree $r-1$. Furthermore,

$$f_1(x) = (1 + x)^2\, \phi(x) \tag{16}$$

characterizes the same FSR as (15), where the feedback is the complementary mod 2 sum (instead of mod 2 sum) and

$$a_k = 1 + a_{k-i} + a_{k-j} + a_{k-r} \tag{17}$$

The length of the longest cycle from (16) is

$$LCM\ [2 \cdot 1,\ 2^{r-1}-1] \text{ or } 2^r - 2$$

From theorem 3, the FSR associated with (16) and (17) has an even number of cycles. Clearly this means there can only be *two* cycles, one of length 2^r-2 and one of length 2. The only sequence of length 2 is (01), and it corresponds to the factor $(1 + x)^2$ in $f_1(x)$. The two states of the length 2 cycle are as follows:

Stage	1 2 3 4 · · · r	k	a_k
	0 1 0 1 · · · ·	0	1
	1 0 1 0 · · · ·	1	0

Case 1 $r \equiv 0 \bmod 2$

$$a_k = a_{k-r} = 1 + a_{k-i} + a_{k-j} + a_{k-r}$$

$$a_{k-i} + a_{k-j} = 1$$

Thus

$$i + j \equiv 1 \bmod 2$$

$$r \equiv 0 \bmod 2$$

and $i + j + r \equiv 1 \bmod 2$.

Case 2 $r \equiv 1 \bmod 2$

$$a_k = 1 + a_{k-r} = 1 + a_{k-i} + a_{k-j} + a_{k-r}$$

$$a_{k-i} + a_{k-j} = 0$$

Thus

$$i + j \equiv 0 \bmod 2$$

$$r \equiv 1 \bmod 2$$

and $i + j + r \equiv 1 \bmod 2$.

Therefore, (14) must be satisfied for a cycle of length 2 to exist. This does not guarantee that a cycle of length 2^r-2 will also exist. However, it follows that a cycle of length $2^r - 2$ cannot exist and $\phi(x)$ in (15) is not primitive if (14) is not satisfied.

THEOREM 6. *A necessary but not sufficient condition for a tetranomial $1 + x^i + x^j + x^r$ to have a period $2^{r-1}-2$ is that*

$$i + j + r \equiv 0 \bmod 4 \tag{18}$$

Proof. If $f_0(x) = 1 + x^i + x^j + x^r$ has period $2^{r-1}-2$, then

$$f_0(x) = (1+x)^2\,\theta(x) \tag{19}$$

where $\theta(x)$ is a primitive polynomial of degree $r-2$. Furthermore,

$$f_1(x) = (1+x)^3\,\theta(x) \tag{20}$$

characterizes the same FSR as (19), where the feedback is the complementary mod 2 sum (instead of mod 2 sum).

The length of the longest cycle from (20) is

$$LCM\,[4 \cdot 1, 2^{r-2}-1] = 2^r - 4$$

From theorem 3, the FSR associated with (19) has an even number of cycles. The complementary mod 2 sum feedback cannot yield either of the two possible sequences (0) or (1) of length 1. Thus the remaining four states must lie on a cycle of length 4. The factor $(1+x)^3$ of $f_1(x)$ corresponds to the sequence (0011). The four states of the length 4 cycle are:

Stage	1 2 3 4 5 · · · r	k	a_k
	0 0 1 1 0 · · · ·	0	1
	1 0 0 1 1 · · · ·	1	1
	1 1 0 0 1 · · · ·	2	0
	0 1 1 0 0 · · · ·	3	0

If $j - i = 0 \bmod 4$, then $a_{k-i} = a_{k-j}$. If $j - i \equiv 2 \bmod 4$, then $a_{k-i} = 1 + a_{k-j} = a'_{k-1}$.

There are four cases to be considered, as follows:

Case 1 $r \equiv 0 \bmod 4$

$$a_k = a_{k-r} = 1 + a_{k-i} + a_{k-j} + a_{k-r}$$

$$a_{k-i} + a_{k-j} = 1$$

Thus

$$j - i \equiv 2 \bmod 4$$

and i and j are both odd or both even. The latter must be ruled out since this would mean that

$$f_0(x) = 1 + x^{2i_1} + x^{2j_1} + x^{2r_1} = (1 + x^{i_1} + x^{j_1} + x^{r_1})^2$$

Therefore,

$$i = 2q_1 - 1$$

$$j = 4q_2 + 2q_1 + 1$$

$$r = 4q_3$$

and $i + j + r = 4(q_1 + q_2 + q_3) \equiv 0 \bmod 4$.

Case 2 $r \equiv 1 \bmod 4$

$a_k = 1 + a_{k-2}$ and $a_{k-r} = a_{k-1}$

Thus

$$1 + a_{k-2} = 1 + a_{k-i} + a_{k-j} + a_{k-1}$$

$$a_{k-1} + a_{k-2} + a_{k-i} + a_{k-j} = 0$$

If

$$i \neq 1, 2 \text{ and } j \neq 2.$$

Solution 1

$$i - 1 \equiv 0 \bmod 4$$

$$j - 2 \equiv 0 \bmod 4$$

and $i + j + r \equiv 0 \bmod 4$.

Solution 2

$$i - 1 \equiv 2 \bmod 4$$

$$j - 2 \equiv 2 \bmod 4$$

and $i + j + r \equiv 0 \bmod 4$.

The foregoing holds for $i \longleftrightarrow j$.

If $i = 1$,

$$a_{k-2} + a_{k-j} = 0$$

$$j - 2 \equiv 0 \bmod 4$$

and $i + j + r \equiv 0 \bmod 4$.

If $i = 2$,

$$a_{k-1} + a_{k-j} = 0$$

$$j - 1 \equiv 0 \bmod 4$$

and $i + j + r \equiv 0 \bmod 4$

If $j = 2$, $i = 1$, since $i < j$ and $i + j + r \equiv 0 \bmod 4$.

The proof for case 3, where $r \equiv 2 \bmod 4$, parallels that for case 1. Also the proof for case 4, where $r \equiv 3 \bmod 4$, parallels that of case 2.

Thus if (18) is not satisfied, $f_0(x)$ in (19) could not contain $\theta(x)$ as a factor where $\theta(x)$ is primitive and of degree $r - 2$.

The search is further reduced by noting that the period of a given tetranomial is the same as that of its reciprocal. The tetranomial

$$x^{r-0} + x^{r-i} + x^{r-j} + x^{r-r} = x^r + x^{r-i} + x^{r-j} + 1$$

is the reciprocal of $x^r + x^j + x^i + 1$. Also, cases can be discarded where either i, j, or r is a multiple of 3 (say $i \equiv 0 \bmod 3$) and the remaining two exponents are congruent mod 3 (i.e., $j \equiv r \bmod 3$). When the preceding holds, $f_0(x)$ contains $1 + x + x^2$ as a factor (Ref. 3).

The results of the search appear in Tables 1 and 2 through degree 34.

III. Conclusions

Tetranomials of the form

$$f_0(x) = 1 + x^i + x^j + x^r = (1 + x)\phi(x)$$

with period $2^{r-1}-1$ exist for every degree r, $4 \leq r \leq 34$, with the exception of degree 13. Each of these contains $\phi(x)$ as a factor where $\phi(x)$ is a primitive polynomial of degree $r - 1$. Dividing each rth-degree tetranomial corresponding to an entry in Table 1 by $x + 1$ thus yields a *primitive polynomial* over $GF(2)$ of degree $r - 1$. Furthermore a maximal-length PN sequence of period $2^{r-1}-1$ can be generated for every $r - 1$ (excluding $r - 1 = 12$), with an r-stage three-tap FSR. An initial state of $11 \cdots 10$ yields a PN sequence associated with the characteristic polynomial $\phi(x)$, whereas an initial state of $00 \cdots 01$ yields a complementary PN sequence associated with the characteristic polynomial $(1 + x)\ \phi(x)$ (see theorem 4).

Tetranomials of the form

$$f_0(x) = 1 + x^i + x^j + x^r$$
$$= (1 + x)^2\,\theta(x)$$

with periods $2^{r-1}-2$ exist for every degree r, $4 \leq r \leq 34$, with the exceptions of degrees 6, 8, and 14. Each of these contains $\theta(x)$ as a factor, where $\theta(x)$ is a primitive polynomial of degree $r - 2$. Dividing each rth-degree tetranomial corresponding to an entry in Table 2 by $x^2 + 1$ thus yields a *primitive polynomial* over $GF(2)$ of degree $r - 2$. Furthermore, a sequence of length $2^{r-1}-2$ can be generated for every $r - 1$ (excluding $r - 1 = 5$, 7, and 13). The initial state $00 \cdots 01$ lies on the cycle of length $2^{r-1}-2$. Two cycles that are complementary images of one another correspond to $(1 + x)\ \theta(x)$ and $\theta(x)$, respectively. Each yields PN sequences of length $2^{r-2}-1$. The remaining cycles yield two sequences of length 1: namely, (0) and (1) corresponding to $(1 + x)$ and the sequence of length 2 corresponding to $1 + x^2$.

Example 3. Consider $f_0(x) = 1 + x + x^2 + x^5$. The six disjoint cycles are tabulated as follows:

k	a_1	a_2	a_3	a_4	a_5	a_k	a_1	a_2	a_3	a_4	a_5	a_k
0	0	0	0	0	1	1	0	1	0	1	0	1
1	1	0	0	0	0	1	1	0	1	0	1	0
2	1	1	0	0	0	0						
3	0	1	1	0	0	1						
4	1	0	1	1	0	1						
5	1	1	0	1	1	1						
6	1	1	1	0	1	1						
7	1	1	1	1	0	0						
8	0	1	1	1	1	0						
9	0	0	1	1	1	1						
10	1	0	0	1	1	0						
11	0	1	0	0	1	0						
12	0	0	1	0	0	0						
13	0	0	0	1	0	0						
0	1	1	0	1	0	0	0	0	1	0	1	1
1	0	1	1	0	1	0	1	0	0	1	0	1
2	0	0	1	1	0	0	1	1	0	0	1	1
3	0	0	0	1	1	1	1	1	1	0	0	0
4	1	0	0	0	1	0	0	1	1	1	0	1
5	0	1	0	0	0	1	1	0	1	1	1	0
6	1	0	1	0	0	1	0	1	0	1	1	0
0	0	0	0	0	0	0	1	1	1	1	1	1

The sequences of length 7 are PN sequences. Note that

$$f_0(x) = 1 + x + x^2 + x^5$$
$$= (1 + x)^2(1 + x + x^3)$$

where $\theta(x) = 1 + x + x^3$ and is primitive.

Associated with every r-stage FSR corresponding to feedback configurations in Table 2 are complementary disjoint cycles of states which yield PN sequences of length $2^{r-2}-1$ for every $r - 2$ (excluding $r - 2 = 4$, 6,

12). It may be shown that when $r > 4$ the initial state $00 \cdots 0101$ results in a $g_0(x) = 1 + x^2$ and lies on a cycle of length $2^{r-2}-1$ corresponding to $\theta(x)$. The complementary state $11 \cdots 1010$ lies on a cycle of length $2^{r-2}-1$ (theorem 4) corresponding to $(1 + x)\theta(x)$.

A *primitive trinomial does not exist* of degree $r - 1$ equal to 8, 12, 13, 14, 16, 19, 24, 26, 27, 30, and 32. *Tetranomials* of degree r *do exist*, however, which contain as a factor a *primitive polynomial* $\phi(x)$ of degree $r - 1$ for each of the preceding values of $r - 1$ except 12.

Table 1. Tetranomials $1 + x^i + x^j + x^r$ with periods $2^{r-1}-1$

i	j	r
1	2	4
1	3	5
1	2	6
2	3	
1	5	7
2	4	
1	2	8
1	4	
1	6	
3	4	
2	6	9
3	5	
2	3	10
2	5	
3	6	
1	3	11
2	4	
2	7	12
1	2	14
2	5	
2	7	
2	11	
3	4	
4	9	
5	8	

i	j	r
3	5	15
5	7	
6	8	
1	2	16
1	14	
2	11	
2	13	
3	6	
3	12	
4	5	
4	11	
5	10	
7	8	
1	11	17
4	10	
1	12	18
1	14	
2	7	
2	9	
3	8	
4	5	
4	11	
5	6	
1	7	19
6	12	
7	11	

i	j	r
1	14	20
2	11	
5	14	
1	3	21
1	11	
3	11	
4	6	
4	12	
6	8	
8	10	
1	8	22
1	16	
2	9	
3	12	
4	7	
6	9	
1	21	23
2	8	
2	16	
1	2	24
1	12	
1	18	
2	15	
2	21	
3	8	
3	16	
3	20	
4	17	
5	12	

i	j	r
5	16	24
6	7	
6	13	
7	14	
8	9	
10	11	
2	14	25
5	19	
6	14	
8	14	
1	4	26
1	12	
1	18	
1	22	
2	11	
4	5	
4	15	
5	8	
9	10	
9	12	
9	16	
10	15	
1	5	27
1	15	
2	6	
3	7	
3	11	
5	13	
6	10	

i	j	r
7	11	27
7	17	
2	5	28
5	15	
5	22	
6	15	
6	21	
1	17	29
2	22	
3	15	
3	19	
4	24	
8	20	
11	17	
2	13	30
3	22	
4	11	
4	23	
6	7	
9	16	
11	12	
11	18	
2	12	31
9	21	
1	4	32
1	8	
1	14	

i	j	r
1	24	32
1	28	
2	19	
3	4	
3	6	
3	24	
4	15	
4	19	
4	25	
5	20	
6	7	
6	19	
7	8	
7	12	
9	16	
9	18	
10	13	
11	20	
13	14	
13	16	
2	10	33
4	14	
10	14	
11	19	
1	14	34
2	11	
2	21	
4	13	
9	14	
13	16	

Table 2. Tetranomials $1 + x^i + x^j + x^r$ with periods $2^{r-1} - 2$

i	j	r	i	j	r	i	j	r	i	j	r	i	j	r	i	j	r
1	3	4	1	2	13	5	9	18	2	19	23	9	15	28	3	25	32
			2	9					6	7					5	11	
1	2	5	4	7		2	3	19				1	2	29			
			5	6		2	11		1	3	24	1	10		2	9	33
1	4	7				7	10		5	15		2	17		2	25	
2	3		1	12	15							7	16		7	24	
			2	3		5	7	20	1	22	25	13	14		10	17	
1	2	9	3	10		5	11		3	20							
1	6		4	5					7	16		5	9	30	1	13	34
						1	2	21	8	15					1	29	
1	5	10	1	7	16	1	6					1	8	31			
						7	12		1	17	26	2	27				
1	4	11	1	14	17				3	19		3	6				
3	6		3	4		1	13	22				3	26				
4	5		3	12		3	15		1	20	27	5	24				
			6	9					2	3		7	22				
1	3	12				2	11	23	9	16		9	12				

References

1. Carmichael, R. D., *Introduction to the Theory of Groups of Finite Order,* Dover Publications, New York, 1956.
2. Hardy, G. H., and Wright, E. M., *An Introduction to the Theory of Numbers,* Oxford University Press, Amen House, London, 1958.
3. Golomb, S. W., *Shift Register Sequences,* Holden-Day, Inc., San Francisco, 1967.
4. Gilbert, E. N., *Quasi-Random Binary Sequences,* Bell Telephone Laboratories Memorandum MM-53-1400-42, Nov. 27, 1953.
5. Marsh, R. W., *Table of Irreducible Polynomials over GF(2) Through Degree 19,* National Security Agency, Washington, D.C., Oct. 24, 1957.
6. Peterson, W. W., *Error-Correcting Codes,* John Wiley and Sons, New York, 1961.
7. Watson, E. J., "Primitive Polynomials (Mod 2)," *Math.*, Vol. 16, pp. 368–369, 1962.
8. Zierler, N., and Brillhart, J., "On Primitive Trinomials," *Inform. Contr.*, Vol. 13, pp. 541–554, 1968.
9. Swan, R. G., "Factorization of Polynomials over Finite Fields," *Pac. J. Math.*, Vol. 12, pp. 1099–1106, 1962.
10. Hall, M. Jr., *Combinatorial Theory,* Blaisdell Pub. Co., Waltham, Mass., 1967.