

General Disclaimer

One or more of the Following Statements may affect this Document

- This document has been reproduced from the best copy furnished by the organizational source. It is being released in the interest of making available as much information as possible.
- This document may contain data, which exceeds the sheet parameters. It was furnished in this condition by the organizational source and is the best copy available.
- This document may contain tone-on-tone or color graphs, charts and/or pictures, which have been reproduced in black and white.
- This document is paginated as submitted by the original source.
- Portions of this document are not fully legible due to the historical nature of some of the material. However, it is the best reproduction available from the original submission.

JPL Publication 85-7

(NASA-CR-175649) PERIODIC BINARY SEQUENCE
GENERATORS: VLSI CIRCUITS CONSIDERATIONS
(Jet Propulsion Lab.) 200 F HC A09/HF A01

N85-22886

CSCI 09C

Unclas

G3/33

14806

Periodic Binary Sequence Generators: Very Large Scale Integrated (VLSI) Circuits Considerations

Marvin Periman



December 1984

NASA

National Aeronautics and Space Administration

Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

Periodic Binary Sequence Generators: Very Large Scale Integrated (VLSI) Circuits Considerations

Marvin Perlman

December 1984



National Aeronautics and Space Administration

Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

The research described in this publication was carried out by the Jet Propulsion Laboratory, California Institute of Technology, under contract with the National Aeronautics and Space Administration, NASA Task RE-210.

ABSTRACT

Feedback shift registers have proven to be efficient periodic binary sequence generators. Polynomials of degree r over a Galois field characteristic 2 ($GF(2)$) characterize the behavior of shift registers with linear-logic feedback.

The object of this report is the algorithmic determination of the trinomial of lowest degree, when it exists, that contains a given irreducible polynomial over $GF(2)$ as a factor. This corresponds to embedding the behavior of an r -stage shift register with linear-logic feedback into that of an n -stage shift register with a single two-input modulo 2 summer (i.e., Exclusive-OR gate) in its feedback. This leads to Very Large Scale Integrated (VLSI) circuit architecture of maximal regularity (i.e., identical cells) with intercell communications serialized to a maximal degree.

ACRONYMS

Cp	clock pulse
CP	Compatible Pair
CPI	Clock Pulse Interval
FSR	Feedback Shift Register
GF	Galois Field
ISFSR	shift register with interstage feedback
LCM	Least Common Multiple
MOSFET	Metal-Oxide-Semiconductor Field-Effect Transistor
NMOS	N Channel Metal-Oxide Semiconductor
PN	Pseudonoise
SSFSR	shift register with single stage feedback
VLSI	Very Large Scale Integrated circuits

~~PRECEDING PAGE BLANK NOT FILMED~~

CONTENTS

I. BACKGROUND 1-1

II. GENERATORS OF PERIODIC BINARY SEQUENCES 2-1

 A. FEEDBACK SHIFT REGISTERS 2-1

 B. FEEDBACK SHIFT REGISTERS CHARACTERIZED BY
 RECURRENCE RELATIONS 2-8

III. AN ISOMORPHISM BETWEEN THE STATES OF AN r -STAGE
 SSFSR AND AN r -STAGE ISFSR 3-1

IV. THE EXISTENCE AND ALGORITHMIC DETERMINATION OF A TRINOMIAL
 OF LEAST DEGREE THAT CONTAINS A GIVEN IRREDUCIBLE
 POLYNOMIAL OVER $GF(2)$ AS A FACTOR 4-1

 A. PRIMITIVE POLYNOMIALS OVER $GF(2)$ 4-1

 B. IRREDUCIBLE NONPRIMITIVE POLYNOMIALS OVER $GF(2)$ 4-33

V. VERY LARGE SCALE INTEGRATED CIRCUIT CONSIDERATIONS 5-1

VI. SUMMARY 6-1

VII. REFERENCES 7-1

APPENDIXES

 A. NUMBER-THEORETIC FUNCTIONS A-1

 B. TRINOMIAL OF LEAST DEGREE THAT CONTAINS A GIVEN
 PRIMITIVE POLYNOMIAL OF DEGREE r OVER $GF(2)$ AS A FACTOR B-1

 C. TRINOMIAL OF LEAST DEGREE THAT CONTAINS A GIVEN
 IRREDUCIBLE NONPRIMITIVE POLYNOMIAL OF DEGREE r OVER
 $GF(2)$ AS A FACTOR C-1

PRECEDING PAGE BLANK NOT FILMED

Figures

2-1. Functional Logic Diagram of a Feedback Shift Register that Performs Multiplication by α Modulo $\alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1$ 2-2

2-2. Functional Logic Diagram of a Feedback Shift Register that Performs Division by α Modulo $\alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1$ 2-4

2-3. Functional Logic Diagram of an r-stage Shift Register with Linear Logic Feedback (SSFSR) 2-9

3-1. A 4-Stage SSFSR and a 4-Stage ISFSR with Isomorphic State Spaces 3-5

3-2. The One-to-One Correspondence Between $d_{k-1}d_{k-2}d_{k-3}$ and $b_2y^2 + b_1y + 1$ 3-19

3-3. An SSFSR and its Corresponding ISFSR of Identical Complexity 3-37

4-1. (a) A 31-bit PN Sequence, (b) its Run Length Properties, (c) Closure Illustrated in the Isomorphic Abelian Group . . 4-6

5-1. Master-Slave O-Enable JK Flip-Flop 5-2

5-2. NMOS Circuit of a Static O-Enable JK Flip-Flop 5-7

5-3. A Functional Logic Diagram of a n-Stage SSFSR Characterized by $X^n + X^a + 1$ 5-8

Tables

1-1. $GF(2^6)$ Generated by α , a Root of $f(x) = x^6 + x^5 + x^2 + x + 1$, with α^* Adjoined 1-3

1-2. Irreducible Factors of $x^{2^6-1} - 1$ Over $GF(2)$ 1-8

1-3. Elements Generated by β , a Root of $f(x) = x^6 + x^5 + x^4 + x^2 + 1$ 1-10

1-4. Irreducible Factors of $x^{2^1} - 1$ Over $GF(2)$ 1-12

1-5. Irreducible Self-Reciprocal Factors of $X^{513} - 1$ Over $GF(2)$ Enumerated by the Order of their Roots and their Degree 1-19

2-1. Equal Length FSR Cycles of (nonzero) States Corresponding to the Decomposition of a Multiplicative Group into a Cyclic Subgroup $\{\beta^i\}$ and Cosets $\{\gamma\beta^j\}$ and $\{\delta\beta^k\}$ 2-7

2-2.	State Table of a 7-Stage SSFSR and Components of a Decomposition for $f(x) = 1 + x + x^3 + x^4 + x^7$ $= (1 + x^2 + x^3)(1 + x + x^2 + x^3 + x^4)$	2-21
2-3.	Initial States of a 7-Stage SSFSR that Map onto a $g(x)$ Containing $x^4 + x^3 + x^2 + x + 1$ as a Factor	2-28
3-1.	The One-to-One Correspondence Between the States of an SSFSR and the $g(x)$ Polynomials	3-2
3-2.	Cycle Structure and Isomorphism of SSFSR and ISFSR States Whose Respective Next State Transformations are Affine . . .	3-23
4-1	A 63-State Cycle Associated with $x^6 + x^5 + x^2 + x + 1$ a Factor of $x^{11} + x^8 + 1$	4-18

SECTION I

BACKGROUND

The root α of a primitive polynomial $f(x)$ is a generator of the cyclic group

$$\alpha, \alpha^2, \dots, \alpha^{2^r-2}, \alpha^{2^r-1} = 1$$

The $2^r - 1$ elements of the multiplicative group with the element 0 adjoined are members of a Galois Field of order 2^r (i.e., $GF(2^r)$). The elements 0 and 1 comprise $GF(2)$, a subfield of $GF(2^r)$, and $GF(2^r)$ is a finite extension of $GF(2)$.

Each element in $GF(2^r)$ satisfies

$$x^{2^r} - x = x(x^{2^r-1} - 1) = 0$$

The element 0 satisfies $x = 0$ and each of the nonzero elements satisfies

$$x^{2^r-1} - 1 = 0$$

Example 1

Consider the primitive polynomial $GF(2)$

$$f(x) = x^6 + x^5 + x^2 + x + 1$$

with one of 6 distinct roots denoted by α . Every nonzero element in $GF(2^6)$ is expressible as an integer power of α .

$$\alpha^j = b_5\alpha^5 + b_4\alpha^4 + b_3\alpha^3 + b_2\alpha^2 + b_1\alpha + b_0$$

where $b_i \in GF(2)$ and α^j is among the $2^r - 1$ roots of unity. The polynomial in α is of degree 5 or less since

$$\alpha^6 = \alpha^5 + \alpha^2 + \alpha + 1$$

The element 0 is the constant zero polynomial denoted by

$$\alpha^* = 0 \cdot \alpha^5 + 0 \cdot \alpha^4 + \dots + 0$$

Members of $GF(2^6)$, generated by α with α^* adjoined, appear in Table 1-1.

The binary operation of "addition" defined on the field elements is termwise sum modulo 2 (i.e., vector addition over $GF(2)$).

For example,

$$\begin{array}{r} 1\ 1\ 1\ 1\ 0\ 0\ (\alpha^{14}) \\ +\ 1\ 1\ 0\ 1\ 1\ 1\ (\alpha^{54}) \\ \hline 0\ 0\ 1\ 0\ 1\ 1\ (\alpha^{19}) \end{array}$$

The binary operation of "multiplication" on the field elements is defined as

$$(b_5\alpha^5 + b_4\alpha^4 + \dots + b_0) (d_5\alpha^5 + d_4\alpha^4 + \dots + d_0)$$

with the result reduced modulo

$$f(\alpha) = \alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1$$

Since each element is expressible as a power of α ,

$$\alpha^i \alpha^j = \alpha^{(i+j) \bmod 63}$$

Table 1-1. GF(2⁶) Generated by α , a Root of $f(x) = x^6 + x^5 + x^2 + x + 1$,
with α^* Adjoined

i of α^i	b_5	b_4	b_3	b_2	b_1	b_0	i of α^i	b_5	b_4	b_3	b_2	b_1	b_0
*	0	0	0	0	0	0	31	0	0	1	1	1	0
0	0	0	0	0	0	1	32	0	1	1	1	0	0
1	0	0	0	0	1	0	33	1	1	1	0	0	0
2	0	0	0	1	0	0	34	0	1	0	1	1	1
3	0	0	1	0	0	0	35	1	0	1	1	1	0
4	0	1	0	0	0	0	36	1	1	1	0	1	1
5	1	0	0	0	0	0	37	0	1	0	0	0	1
6	1	0	0	1	1	1	38	1	0	0	0	1	0
7	1	0	1	0	0	1	39	1	0	0	0	1	1
8	1	1	0	1	0	1	40	1	0	0	0	0	1
9	0	0	1	1	0	1	41	1	0	0	1	0	1
10	0	1	1	0	1	0	42	1	0	1	1	0	1
11	1	1	0	1	0	0	43	1	1	1	1	0	1
12	0	0	1	1	1	1	44	0	1	1	1	0	1
13	0	1	1	1	1	0	45	1	1	1	0	1	0
14	1	1	1	1	0	0	46	0	1	0	0	1	1
15	0	1	1	1	1	1	47	1	0	0	1	1	0
16	1	1	1	1	1	0	48	1	0	1	0	1	1
17	0	1	1	0	1	1	49	1	1	0	0	0	1
18	1	1	0	1	1	0	50	0	0	0	1	0	1
19	0	0	1	0	1	1	51	0	0	1	0	1	0
20	0	1	0	1	1	0	52	0	1	0	1	0	0
21	1	0	1	1	0	0	53	1	0	1	0	0	0
22	1	1	1	1	1	1	54	1	1	0	1	1	1
23	0	1	1	0	0	1	55	0	0	1	0	0	1
24	1	1	0	0	1	0	56	0	1	0	0	1	0
25	0	0	0	0	1	1	57	1	0	0	1	0	0
26	0	0	0	1	1	0	58	1	0	1	1	1	1
27	0	0	1	1	0	0	59	1	1	1	0	0	1
28	0	1	1	0	0	0	60	0	1	0	1	0	1
29	1	1	0	0	0	0	61	1	0	1	0	1	0
30	0	0	0	1	1	1	62	1	1	0	0	1	1

Logarithms of field elements to the base α are provided by Table 1-1 to simplify multiplication of nonzero elements as follows:

$$\begin{array}{r}
 \alpha^{49} \quad (1 \ 1 \ 0 \ 0 \ 0 \ 1) \\
 \alpha^{34} \quad (0 \ 1 \ 0 \ 1 \ 1 \ 1) \\
 \hline
 \alpha^{34} \alpha^{49} = \alpha^{20} \quad (0 \ 1 \ 0 \ 1 \ 1 \ 0)
 \end{array}$$

The (multiplicative) order of a nonzero element α in $GF(2^r)$ is the least integer m for which $\alpha^m = 1$. Furthermore, m divides $2^r - 1$, the order of the multiplicative group, in accordance with a corollary of a fundamental theorem due to Lagrange (see Reference 1).

As presented in Reference 2, consider the operation σ which squares each of the roots of

$$g(x) = \prod_{i=1}^r (x - \alpha^i)$$

any polynomial of degree r over $GF(2)$. Noting that

$$-1 \equiv 1 \pmod{2} \text{ and } (a + b)^2 = a^2 + b^2 \text{ over } GF(2),$$

then

$$\begin{aligned}
 [g(x)] &= \prod_{i=1}^r (x - \alpha_i^2) = \prod_{i=1}^r (t^2 - \alpha_i^2) \\
 &= \prod_{i=1}^r (t - \alpha_i)^2 = \left[\prod_{i=1}^r (t - \alpha_i) \right]^2 \\
 &= [g(t)]^2 = g(t^2) = g(x)
 \end{aligned}$$

The substitution $t^2 = x$ is appropriately employed in proving that $g(x)$ over $GF(2)$ is invariant under the operation σ . The root-squaring operation σ on $g(x)$ which leaves $g(x)$ unchanged is termed an automorphism. If in particular $g(x)$ of degree r is irreducible, then $g(x)$ has the following r distinct automorphisms:

$$1, \sigma, \sigma^2, \dots, \sigma^{r-1}$$

with respect to $GF(2^r)$. An operation on a root of $g(x)$ is an automorphism if and only if it is an integer power of σ , the root-squaring operation. Consequently, $g(x)$ has r distinct roots, namely,

$$\alpha, \alpha^2, \alpha^{2^2}, \dots, \alpha^{2^{r-1}}$$

Since σ^r maps α into α^{2^r} and $\alpha^{2^r} = \alpha$ (from $\alpha^{2^r-1} = 1$), σ^r is the identity operation.

The product of all irreducible polynomials over $GF(2)$ whose degrees divide r is $x^{2^r} - x$. Complete factorization is best illustrated by arranging the $2^r - 1$ roots of unity into cyclotomic cosets (see References 2 and 3). Given a primitive polynomial $f(x)$ of degree r over $GF(2)$. Each distinct root is of order $2^r - 1$, hence, a primitive root of unity.

A fundamental property associated with the multiplicative order of field elements is as follows:

If β has order m , then

$$\beta^j \text{ has order } m/(m,j)$$

where (m,j) denotes the greatest common divisor of m and j . Clearly m and $m/(m,j)$ divide $2^r - 1$, the number of nonzero elements in $GF(2^r)$. The integer (m,j) is called the index of the order of β^j . A primitive r^{th}

degree polynomial has α , a primitive root of unity, as a root. Each of the r roots has order $2^r - 1$ since $(2^r - 1, 2^i) = 1$ for all i .

The set of integers

$$\{i\} = \{1, 2, 4, \dots, 2^{r-1}\}$$

taken from the multiplicative group of integers modulo $2^r - 1$ form a subgroup. The corresponding set

$$\{\alpha^i\} = \{\alpha, \alpha^2, \alpha^4, \dots, \alpha^{2^{r-1}}\}$$

contains the r distinct roots of $f(x)$. The "generalized cosets"

$$\{iv\} = \{v, 2v, 4v, \dots, (2^r - 1)v\}$$

are nonoverlapping sets which together with the subgroup $\{i\}$, the special coset where $v = 1$, comprise the multiplicative group modulo $2^r - 1$. If $(2^r - 1, v) = 1$, then $\{iv\}$ is a coset as defined in group theory. The elements of such a coset correspond to $r(2^r - 1)$ st primitive roots of unity whose minimal polynomial is a primitive polynomial over $GF(2)$ (see Reference 4). There are $\varphi(2^r - 1)/r$ such cosets (including the subgroup) and, therefore, $\varphi(2^r - 1)/r$ primitive polynomials of degree r over $GF(2)$. The number-theoretic function $\varphi(m)$, known as the Euler phi-function, is the number of positive integers no greater than m (a positive integer) that are relatively prime to m (see Appendix A). The integers a and m are termed relatively prime if $(a, m) = 1$.

An "improper coset" results for values of v where $(2^r - 1, v) \neq 1$. If such a coset contains r distinct elements, the elements correspond to $r(2^r - 1)$ st nonprimitive roots of unity whose minimal polynomial is an irreducible nonprimitive r th degree polynomial over $GF(2)$. Whereas the elements of a coset containing $s < r$ distinct elements (where s necessarily divides r) correspond to $s(2^B - 1)$ st roots of unity whose minimal polynomial is an irreducible polynomial of degree s over $GF(2)$.

The product of the minimal polynomials associated with each of the cyclotomic cosets (i.e., generalized cosets which include improper cosets) yields $x^{2^r-1} - 1$. The set of minimal polynomials is comprised of all irreducible polynomials over GF(2) whose degrees divide r.

Example 2

The irreducible factors of $x^{2^6-1} - 1$ over GF(2) are given in Table 1-2. The 63 roots of unity are generated by α , a root of

$$F(x) = x^6 + x^5 + x^2 + x + 1$$

Consider the conjugate roots (i.e., roots of the same minimal polynomial)

$$\alpha^3, \alpha^6, \dots, \alpha^{33}$$

corresponding to the cyclotomic coset

$$\{1 \cdot 3, 2 \cdot 3, \dots, 2^5 \cdot 3\} \text{ mod } 63 = \{3, 6, \dots, 33\}$$

The minimal polynomial for these roots is determined as follows:

$$\begin{aligned} f(\alpha^3) &= (\alpha^3)^6 + d_5(\alpha^3)^5 + d_4(\alpha^3)^4 + d_3(\alpha^3)^3 + d_2(\alpha^3)^2 + d_1(\alpha^3) + 1 = 0 \\ &= \alpha^{18} + d_5\alpha^{15} + d_4\alpha^{12} + d_3\alpha^9 + d_2\alpha^6 + d_1\alpha^3 + 1 = 0 \end{aligned}$$

Substituting entries in Table 1-1 corresponding to the foregoing powers of α gives

Table 1-2. Irreducible Factors of $x^{2^6-1} - 1$ Over GF(2)

Cyclotomic Coset	Minimal Polynomial f(x)	Degree	Index	Order of Roots of f(x)
0	$x + 1$	1	63	1
1 2 4 8 16 32	$x^6 + x^5 + x^2 + x + 1$	6	1	63
3 6 12 24 48 33	$x^6 + x^5 + x^4 + x^2 + 1$	6	3	21
5 10 20 40 17 34	$x^6 + x^5 + x^3 + x^2 + 1$	6	1	63
7 14 28 56 49 35	$x^6 + x^3 + 1$	6	7	9
9 18 36	$x^3 + x + 1$	3	9	7
11 22 44 25 50 37	$x^6 + x^5 + 1$	6	1	63
13 26 52 41 19 38	$x^6 + x + 1$	6	1	63
15 30 60 57 51 39	$x^6 + x^4 + x^2 + x + 1$	6	3	21
21 42	$x^2 + x + 1$	2	21	3
23 46 29 58 53 43	$x^6 + x^4 + x^3 + x + 1$	6	1	63
27 54 45	$x^3 + x^2 + 1$	3	9	7
31 62 61 59 55 47	$x^6 + x^5 + x^4 + x + 1$	6	1	63

$$\begin{array}{r}
[1 1 0 1 1 0] \\
+ d_5 [0 1 1 1 1 1] \\
+ d_4 [0 0 1 1 1 1] \\
+ d_3 [0 0 1 1 0 1] \\
+ d_2 [1 0 0 1 1 1] \\
+ d_1 [0 0 1 0 0 0] \\
+ [0 0 0 0 0 1] \\
\hline
= [0 0 0 0 0 0]
\end{array}$$

The scalar multipliers, d_1 through d_5 , are elements in $GF(2)$. They represent unknowns in determining the linearly independent set of polynomials (i.e., field elements). In this example,

$$d_5 = d_4 = d_2 = 1 \text{ and } d_3 = d_1 = 0$$

The minimal polynomial containing α^3 as a root (as well as $\alpha^6, \dots, \alpha^{33}$) is

$$x^6 + x^5 + x^4 + x^2 + 1$$

The order of α^3 (and its conjugates) is 21. Thus, α^3 is a generator of 21 of the 63 roots of $x^{63} - 1 = 0$ and is a nonprimitive root of unity. The minimal polynomial is, therefore, an irreducible nonprimitive polynomial of degree 6.

The 21 elements generated by $\beta \leftrightarrow \alpha^3$ are tabulated in Table 1-3 where

$$\beta^6 = \beta^5 + \beta^4 + \beta^2 + 1$$

A one-to-one correspondence exists between β^i and α^{3i} (see Table 1-1). Furthermore,

$$\beta^i \beta^j = \beta^{(i+j) \bmod 21} \leftrightarrow \alpha^{3(i+j) \bmod 63} = \alpha^{3i} \alpha^{3j}$$

Table 1-3. Elements Generated by β , a Root of $f(x) = x^6 + x^5 + x^4 + x^2 + 1$

i of β^i	c_5	c_4	c_3	c_2	c_1	c_0
0	0	0	0	0	0	1
1	0	0	0	0	1	0
2	0	0	0	1	0	0
3	0	0	1	0	0	0
4	0	1	0	0	0	0
5	1	0	0	0	0	0
6	1	1	0	1	0	1
7	0	1	1	1	1	1
8	1	1	1	1	1	0
9	0	0	1	0	0	1
10	0	1	0	0	1	0
11	1	0	0	1	0	0
12	1	1	1	1	0	1
13	0	0	1	1	1	1
14	0	1	1	1	1	0
15	1	1	1	1	0	0
16	0	0	1	1	0	1
17	0	1	1	0	1	0
18	1	1	0	1	0	0
19	0	1	1	1	0	1
20	1	1	1	0	1	0

and the two sets $\{\beta^i\}$ and $\{\alpha^{3i}\}$ are isomorphic groups under the defined operation of "multiplication." However, the 21 elements generated by $\beta \longleftrightarrow \alpha^3$ with 0 adjoined do not form a group under the defined operation of addition. Clearly

$$\beta^6 + \beta^5 + \beta^4 + \beta^2 + 1 = \beta^{21} - 1 = 0$$

and

$$x^6 + x^5 + x^4 + x^2 + 1 \text{ divides } x^{21} - 1$$

A fundamental theorem states that $x^d - 1$ divides $x^n - 1$ over any field if and only if d divides n . Thus,

$$x^{21} - 1 \text{ divides } x^{63} - 1$$

is another way of stating that the 21 roots of unity generated by $\beta \mapsto \alpha^3$ are among the 63 roots of unity in $GF(2^6)$.

The roots of

$$x^{2^r-1} - 1 = 0$$

are the nonzero elements in $GF(2^r)$. If s divides r , $2^s - 1$ divides $2^r - 1$ and

$$x^{2^s-1} - 1 \text{ divides } x^{2^r-1} - 1$$

and the roots of

$$x^{2^s-1} - 1 = 0$$

are the nonzero elements of the subfields $GF(2^s)$ in $GF(2^r)$.

In Example 2, $GF(2^6)$ contains the subfields $GF(2^2)$ and $GF(2^3)$. $GF(2)$ is a subfield of $GF(2^2)$ and $GF(2^3)$ as well as of $GF(2^6)$. Although the 21 roots of unity with 0 adjoined do not form a finite field (i.e., 21 is not of the form $2^s - 1$), they contain $GF(2)$, $GF(2^2)$, and $GF(2^3)$.

Example 3

The irreducible factors of $x^{21} - 1$ are given in Table 1-4. The set of integers

$$\{i\} = \{1, 2, 4, 8, 16, 11\}$$

Table 1-4. Irreducible Factors of $x^{21} - 1$ Over $GF(2)$

Cyclotomic Coset	Minimal Polynomial $f(x)$	Degree	Index	Order of Roots of $f(x)$
0	$x + 1$	1	21	1
1 2 4 8 16 11	$x^6 + x^5 + x^4 + x^2 + 1$	6	1	21
3 6 12	$x^3 + x + 1$	3	3	7
5 10 20 19 17 13	$x^6 + x^4 + x^2 + x + 1$	6	1	21
7 14	$x^2 + x + 1$	2	7	3
9 18 15	$x^3 + x^2 + 1$	3	3	7

taken from the multiplicative group of integers modulo 21 form a subgroup. The corresponding set

$$\{\beta^i\} = \{\beta, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^{11}\}$$

are the six distinct roots of

$$f(x) = x^6 + x^5 + x^4 + x^2 + 1$$

The index of each of the 21 roots of unity $\{\beta^j\}$ is relative to 21, the order of $\beta \leftrightarrow \alpha^3$ (i.e., the generator in Table 1-3). Whereas the index of corresponding elements in $\{\alpha^{3j}\}$ (a subset of the 63 roots of unity) is relative to 63, the order of α (i.e., the generator in Table 1-2).

The number of irreducible polynomials over $GF(2)$ of degree 6 whose roots have order 21 is

$$\varphi(21)/6 = \varphi(3)\varphi(7)/6 = 2$$

That is, the order of 12 of the 21 roots of unity are relatively prime to 21 (and, thus, have an index of 1). These elements correspond to two complete

cyclotomic cosets with six members each. Each set of elements are roots of a minimal, hence irreducible, polynomial of degree 6.

In general, if β has order $d < 2^r - 1$ and d divides $2^k - 1$ for $k = r$, but does not divide $2^k - 1$ for $k < r$, then β is a root of a nonprimitive irreducible polynomial over $GF(2)$ of degree r .

Consider the two polynomials of degree r over $GF(2)$:

$$f(x) = x^r + b_{r-1}x^{r-1} + \dots + b_{r-i}x^{r-i} + \dots + b_1x + 1$$

$$g(x) = x^r + b_1x^{r-1} + \dots + b_ix^{r-i} + \dots + b_{r-1}x + 1$$

The coefficient string of one is the reverse of the other.

$$f(x) = \sum_{i=0}^r b_i x^i \qquad g(x) = \sum_{i=0}^r b_{r-i} x^i$$

where b_0 and b_r are necessarily equal to 1 and

$$f(0) = g(0) = 1$$

Thus, $x = \alpha^* = 0$ is not a root of $f(x)$ or $g(x)$.

An equivalent expression for $g(x)$ is

$$g(x) = x^r f(1/x)$$

The polynomial $g(x)$ is defined to be the reciprocal polynomial of $f(x)$ and vice versa. If α is a root of $f(x)$, then α^{-1} (the multiplicative inverse of α) is a root of $g(x)$.

$$g(\alpha^{-1}) = \alpha^{-r} f(\alpha) = 0$$

The transformation

$$f(x) \longleftrightarrow x^r f(1/x)$$

preserves the order of the roots as well as the degree. If α has order n , then $\alpha^{-1} = \alpha^{n-1}$ has order

$$n/(n-1, n) = n$$

A polynomial $f(x)$ of degree r over $GF(2)$ where

$$f(x) = x^r f(1/x)$$

is defined to be self-reciprocal.

Example 4

There are a total of nine irreducible polynomials of degree 6 over $GF(2)$ (see Table 1-2).

Six of the nine are primitive and comprised of three reciprocal pairs. One such pair of polynomials and their corresponding roots are

$$x^6 + x^5 + x^3 + x^2 + 1$$

$$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{17}, \alpha^{34}$$

$$x^6 + x^4 + x^3 + x + 1$$

$$\alpha^{23}, \alpha^{46}, \alpha^{29}, \alpha^{58}, \alpha^{53}, \alpha^{43}$$

The multiplicative inverse of each root in one set is contained in the other, e.g.,

$$(\alpha^5)^{-1} = \alpha^{-5} = \alpha^{63-5} = \alpha^{58}$$

The two nonprimitive polynomials whose roots have order 21 are reciprocal polynomials.

The nonprimitive polynomial whose roots have order 9, namely,

$$x^6 + x^3 + 1$$

is a self-reciprocal polynomial as implied by its corresponding cyclotomic coset. (If α is a root, so is α^{-1} .)

$$\{7, 14, 28, 56, 49, 35\} = \{7, 14, 28, -7, -14, -28\}$$

Reducible self-reciprocal polynomials contain as factors irreducible self-reciprocal polynomial(s) and/or irreducible reciprocal pairs of polynomials. The factors of $x^{53} - 1$, in particular, and $x^n - 1$, in general, are examples. Irreducible self-reciprocal polynomials are of even degree ($r = 2m$) with one exception (i.e., $x + 1$). Their coefficient strings are of the following form:

$$1 \ b_1 \ b_2 \ \dots \ b_{m-1} \ 1 \ b_{m-1} \ \dots \ b_2 \ b_1 \ 1$$

The coefficients of x^{2m} , x^m and x^0 are 1 and each b_i ($1 \leq i < m$) is 0 or 1 (an element of $GF(2)$). Such a coefficient string is of odd weight (i.e., contains an odd number of one's). Thus, the corresponding $f(x)$ cannot contain $x + 1$ as a factor. Being of even degree and having the foregoing coefficient string are necessary, but not sufficient conditions for $f(x)$ to be an irreducible self-reciprocal polynomial.

Assume the cyclotomic coset

$$(1, 2, \dots, 2^{m-1}, 2^m, 2^{m+1}, \dots, 2^{2m-1})$$

corresponds to the roots of a primitive polynomial of degree $2m$. To be self-reciprocal, the following congruence relationship must hold:

$$2^m \equiv -1 \pmod{2^{2m} - 1}$$

Applying rules of modulo arithmetic yields

$$(2^m + 1) \equiv 0 \pmod{2^{2m} - 1}$$

$$(2^m + 1)/(2^{2m} - 1) = q \text{ where } q \text{ is an}$$

integer

and

$$(2^m + 1)/(2^{2m} - 1) = 1/(2^m - 1)$$

Thus, $2^{2m} - 1$ divides $2^m + 1$ only if $m = 1$. It follows that $x^2 + x + 1$ is a self-reciprocal primitive polynomial with roots α and $\alpha^2 = \alpha^{-1}$ of order 3. The only other self-reciprocal primitive polynomial over $GF(2)$ is $x + 1$ whose root is $\alpha^0 = (\alpha^0)^{-1} = 1$ of order 1.

Irreducible nonprimitive self-reciprocal polynomials over $GF(2)$ exist for every even degree greater than 2. Given α of order $2^{2m} - 1$ in $GF(2^{2m})$. The cyclotomic coset

$$\{v, 2v, \dots, 2^{m-1}v, -v, -2v, \dots, -2^{m-1}v\}$$

corresponds to the set of $2m$ distinct roots (which contain α^v) of an irreducible self-reciprocal polynomial of degree $2m$.

$$2^m v \equiv -v \pmod{2^{2m} - 1}$$

$$(2^m + 1)v \equiv 0 \pmod{2^{2m} - 1}$$

$$v \equiv 0 \pmod{(2^{2m} - 1)/(2^m + 1), 2^{2m} - 1}$$

$$v \equiv 0 \pmod{2^m - 1}$$

The $2^m + 1$ solutions are

$$v = s(2^m - 1) \text{ where } 0 \leq s < 2^m + 1$$

and α^v for each v satisfies

$$x^{2^m+1} - 1 = 0$$

The root α^v where $v = 2^m - 1$ has order

$$(2^{2^m} - 1)/(2^m - 1, 2^{2^m} - 1) = 2^m + 1$$

and is a multiplicative generator of the $(2^m + 1)$ st roots of unity. Of these, $\varphi(2^m + 1)$ have order $2^m + 1$, and for $m > 1$, each is a root of one of the $\varphi(2^m + 1)/2m$ irreducible nonprimitive self-reciprocal polynomials. The order of each of the remaining roots divides $2^m + 1$ and is less than $2^m + 1$. Those corresponding to a complete coset (i.e., having $2m$ elements) are roots of a degree $2m$ irreducible nonprimitive self-reciprocal polynomial. Those corresponding to cosets containing fewer than $2m$ elements are roots of an irreducible self-reciprocal polynomial whose degree divides $2m$ and is less than $2m$. Thus, every factor of

$$x^n - 1 \text{ where } n = 2^m + 1$$

is an irreducible self-reciprocal polynomial over $GF(2)$.

Example 5

Given $m = 3$ and $2^m - 1 = 7$. The element α^7 is a generator of the roots of

$$x^n - 1 = 0 \text{ where } n = 2^m + 1 = 9$$

contained in $GF(2^6)$. Each of the roots is a root of an irreducible self-reciprocal polynomial whose degree divides $2m = 6$. The 9 roots represented as v of α^v are

$$\{0, 7, 14, 21, 28, 35, 42, 49, 56\}$$

Following are the minimal polynomials corresponding to each cyclotomic coset:

Cyclotomic Coset	Minimal Polynomial
0	$x + 1$
7 14 28 56(-7) 49(-14) 35(-28)	$x^6 + x^3 + 1$
21 42(-21)	$x^2 + x + 1$

For $m = 9$ and $2^m - 1 = 511$, the element α^{511} is a generator of the roots of $x^{513} - 1 = 0$ contained in $GF(2^{18})$. Included among these roots are the 9 which satisfy

$$x^9 - 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1) = 0$$

each of which is member of $GF(2^{18})$ and one, and only one, of the subfields $GF(2)$, $GF(2^2)$, or $GF(2^6)$.

An enumeration of all the factors (i.e., irreducible self-reciprocal polynomials) of $x^{513} - 1$ by order of their roots and their degree is as follows: Let $\beta = \alpha^{511}$ in $GF(2^{18})$. The order of β^d is

$$n = 513/(d, 513) \text{ where } d = 0, 1, \dots, 512$$

Those values of d that divide $513 = 3^3 \cdot 19$ belong to distinct cyclotomic cosets and may be chosen as representatives (refer to Table 1-5). The last three entries correspond to factors whose roots are also members of a proper subfield of $GF(2^{18})$ (as shown in the first portion of this example).

Table 1-5. Irreducible Self-Reciprocal Factors of $x^{513} - 1$ Over $GF(2)$
 Enumerated by the Order of their Roots and their Degree

d	Order of β^d in $GF(2^{18})$ $n = 513/(d, 513)$	Number of Elements r in Cyclotomic Coset	$\varphi(n)/r$
1	513	18	18
3	171	18	6
9	57	18	2
19	27	18	1
27	19	18	1
57	9	6	1
171	3	2	1
$513 \equiv 0 \pmod{513}$	1	1	1

$\varphi(n)/r$ denotes the number of irreducible self-reciprocal factors of degree r whose roots have order n. The total number of elements with order n (i.e., β^h where $(h, 513) = d$) is equal to $\varphi(n)$.

Finite fields of the same order are isomorphic, and every finite field is isomorphic to a Galois field (Reference 5). Thus, the study of finite fields of order p^r (namely, $GF(p^r)$) where p is a prime integer and r a nonzero positive integer. Each element in $GF(p^r)$ is a polynomial of degree r with coefficients in $GF(p)$ - i.e., 0, 1, ..., or p - 1. Only polynomials in $GF(2^r)$ are discussed due to considerations associated with practical applications.

Example 6

Given γ , a root of the degree 3 primitive polynomial $x^3 + x + 1$. Thus, γ has order 7 and is a (multiplicative) generator of the nonzero elements in $GF(2^3)$.

Refer to Tables 1-1 and 1-2. The degree 6 primitive polynomial, $x^6 + x^5 + x^2 + x + 1$, has α whose order is 63 as a root. Thus, α^9 has order 7 and is a generator of the nonzero elements in the subfield $GF(2^3)$ properly contained in $GF(2^6)$. The minimal polynomial containing α^9 and its conjugates $\{(\alpha^9)^2 \text{ and } (\alpha^9)^4\}$ as roots is $x^3 + x + 1$.

Refer to Tables 1-3 and 1-4. The element $\beta \leftrightarrow \alpha^3$ is a root of the degree 6 irreducible nonprimitive polynomial $x^6 + x^5 + x^4 + x^2 + 1$. The order of β is 21. Whereas, β^6 has order 7 and is a generator of the nonzero elements of $GF(2^3)$, a proper subset of the 21 roots of unity. Furthermore, the minimal polynomial containing $(\beta^3)^2$ and its conjugates $\{\beta^3 \text{ and } (\beta^3)^4\}$ as roots is $x^3 + x + 1$.

Consider the set of elements generated by γ , α^9 , and β^6 , respectively, with 0 adjoined to each set.

i of γ^i	$a_2 a_1 a_0$	j of α^j	$b_5 b_4 b_3 b_2 b_1 b_0$	k of β^k	$c_5 c_4 c_3 c_2 c_1 c_0$
*	0 0 0	*	0 0 0 0 0 0	*	0 0 0 0 0 0
0	0 0 1	0	0 0 0 0 0 1	0	0 0 0 0 0 1
1	0 1 0	9	0 0 1 1 0 1	6	1 1 0 1 0 1
2	1 0 0	18	1 1 0 1 1 0	12	1 1 1 1 0 1
3	0 1 1	27	0 0 1 1 0 0	18	1 1 0 1 0 0
4	1 1 0	36	1 1 1 0 1 1	3	0 0 1 0 0 0
5	1 1 1	45	1 1 1 0 1 0	9	0 0 1 0 0 1
6	1 0 1	54	1 1 0 1 1 1	15	1 1 1 1 0 0

Each set of 8 elements is a different representation of the elements in $GF(2^3)$. The one-to-one correspondence between elements of each set is

$$\gamma^i \leftrightarrow \alpha^{9i} \leftrightarrow \beta^{6i \text{ mod } 21}$$

Multiplication defined on the nonzero elements of each set is as follows:

$$\gamma^i \gamma^j = \gamma^{(i+j) \bmod 7}$$

$$\gamma^7 - 1 = \gamma^3 + \gamma + 1 = 0$$

$$\alpha^i \alpha^j = \alpha^{(i+j) \bmod 63}$$

$$\alpha^{63} - 1 = \alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1 = 0$$

$$(\alpha^9)^7 - 1 = (\alpha^9)^3 + \alpha^9 + 1 = 0$$

$$\beta^i \beta^j = \beta^{(i+j) \bmod 21}$$

$$\beta^{21} - 1 = \beta^6 + \beta^5 + \beta^4 + \beta^2 + 1 = 0$$

$$(\beta^6)^7 - 1 = [(\beta^3)^7 - 1]^2 = 0$$

$$(\beta^3)^7 - 1 = 0$$

$$(\beta^6)^3 + \beta^6 + 1 = [(\beta^3)^3 + \beta^3 + 1]^2 = 0$$

$$(\beta^3)^3 + \beta^3 + 1 = 0$$

The foregoing illustrates that β^3 and $(\beta^3)^2$ are two of the three conjugate roots of $x^3 + x + 1$ a divisor of $x^7 - 1$.



SECTION II

GENERATORS OF PERIODIC BINARY SEQUENCES

A. FEEDBACK SHIFT REGISTERS

The Feedback Shift Register (FSR) in Figure 2-1 stores a representation of the coefficients of the polynomial

$$b_5\alpha^5 + b_4\alpha^4 + b_3\alpha^3 + b_2\alpha^2 + b_1\alpha + b_0$$

Upon the application of the clock pulse (by clocking circuitry not shown), the FSR performs multiplication by α , a root of

$$x^6 + x^5 + x^2 + x + 1 = 0$$

and reduces the result modulo

$$\alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1$$

The content of each register stage is shifted one stage to the left. Overflow resulting when $b_5 = 1$ prior to shifting, represents

$$\alpha^6 = \alpha^5 + \alpha^2 + \alpha + 1$$

which is "vector added" over GF(2) to the shifted contents. Equivalently,

$$\alpha^6 \equiv \alpha^5 + \alpha^2 + \alpha + 1 \pmod{\alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1}$$

The contents of the FSR during two successive Clock Pulse Intervals (CPIs) (i.e., before and after the application of a clock pulse) is illustrated in the following example:

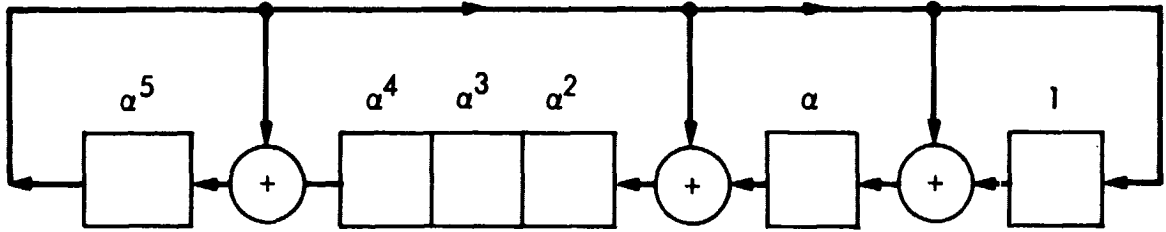


Figure 2-1. Functional Logic Diagram of a Feedback Shift Register that Performs Multiplication by α Modulo $\alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1$

Example 7

$b_5,$	$b_4,$	$b_3,$	$b_2,$	$b_1,$	b_0	at CPI j
$b_4,$	$b_3,$	$b_2,$	$b_1,$	$b_0,$	0	
$b_5,$	0,	0,	$b_5,$	$b_5,$	b_5	
$b_5+b_4,$	$b_3,$	$b_2,$	$b_5+b_1,$	$b_5+b_0,$	b_5	at CPI j+1

In particular,

1 1 0 1 0 1	at CPI j
1 0 1 0 1 0	
1 0 0 1 1 1	
0 0 1 1 0 1	at CPI j + 1
0 1 1 0 1 1	at CPI j
1 1 0 1 1 0	
0 0 0 0 0 0	
1 1 0 1 1 0	at CPI j + 1

The FSR in Figure 2-1 can assume 2^6 or 64 distinct states. The FSR as configured splits the state space into two branchless cycles of states where distinct states have distinct successor states. One cycle is comprised of 63

nonzero states. The succession of these states are identical to those appearing in Table 1-1 where the length of the cycle (i.e., its period) is equal to the order of α . The all zeros state α^* is its own successor state. Thus, it is the single member of a cycle of length 1.

Given a primitive polynomial $f(x)$ over $GF(2)$ of degree $r \geq 2$. The number of terms in $f(x)$ is necessarily odd (i.e., $2m + 1$ where $m \geq 1$). The FSR circuitry that realizes multiplication by α modulo $f(\alpha)$ splits the state space of 2^r binary r -tuples into two disjoint branchless cycles of states. One cycle contains $2^r - 1$ nonzero states identical in representation and sequence of those nonzero elements in $GF(2^r)$ generated by α . The other cycle consists of the singleton all zeros state α^* . The FSR circuitry is comprised of r delay elements (or register stages) and $2m-1$ two-input modulo 2 summers (i.e., Exclusive-OR gates). See References 4 and 6.

Of particular interest are the binary sequences appearing at the output of each register stage. Given the sequence appearing at the output of one stage, the output of each of the other stages is a cyclic permutation of that sequence. The sequence is termed a Pseudonoise (PN) sequence because of its noise-like properties (see Reference 3 and Section IV.A.)

Consider the primitive polynomial

$$f(x) = x^6 + x^5 + x^2 + x + 1$$

where

$$f(\alpha) = \alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1 = 0$$

and

$$\alpha^{-1} = \alpha^5 + \alpha^4 + \alpha + 1$$

The FSR in Figure 2-2 performs division by α (i.e., multiplication by α^{-1}) and reduces the result modulo

$$\alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1$$

The FSR stores a representation of the coefficients of the polynomial

$$b_5\alpha^5 + b_4\alpha^4 + \dots + b_0$$

Upon application of a clock pulse, the content of each register stage is shifted one stage to the right. Overflow resulting when $b_0 = 1$ prior to shifting represents

$$\alpha^{-1} = \alpha^5 + \alpha^4 + \alpha + 1$$

which is vector added over GF(2) to the shifted contents. In terms of congruences

$$\alpha^{-1} \equiv \alpha^5 + \alpha^4 + \alpha + 1 \pmod{\alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1}$$

Note that

$$\alpha^{-1} = 1 \cdot \alpha^{-1} = \alpha^{63-1} = \alpha^{62}$$

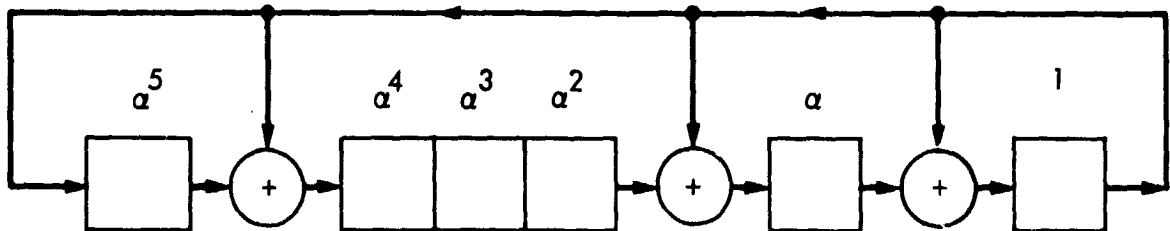


Figure 2-2. Functional Logic Diagram of a Feedback Shift Register that Performs Division by α Modulo $\alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1$

is the last entry in Table 1-1. Successive nonzero states appearing in the register of the FSR in Figure 2-2 are in reverse order of those in Table 1-1. The binary sequence appearing at the output of a given stage of the FSR in Figure 2-2, initialized with a nonzero state, is a PN sequence. It is the reverse of the output of the corresponding stage of the FSR in Figure 2-1, initialized with the same nonzero state.

The element $\beta = \alpha^{-1}$ is a root of

$$g(x) = x^6 + x^5 + x^4 + x + 1$$

where $g(x)$ is the reciprocal polynomial of

$$f(x) = x^6 + x^5 + x^2 + x + 1$$

Thus, an FSR configured to perform multiplication by

$$\beta \text{ modulo } \beta^6 + \beta^5 + \beta^4 + \beta + 1$$

(when initialized with a nonzero state) generates a PN sequence (at the output of each stage). This PN sequence is the reverse of the one generated by the FSR in Figure 2-1. If the FSR is configured to shift from left to right, the states appear in reverse order (of those associated with the FSR in Figure 2-1).

In Example 3, the 6 distinct roots of

$$f(x) = x^6 + x^5 + x^4 + x^2 + 1$$

have order 21, and $f(x)$ is irreducible, but nonprimitive. The 21 roots of unity generated by β , a root of $f(x)$, appear in Table 1-3.

Given an FSR configured to multiply the representation of

$$c_5\beta^5 + c_4\beta^4 + \dots + c_0$$

by β and reduce the result modulo $\beta^6 + \beta^5 + \beta^4 + \beta^2 + 1$. The all zeros state β^* (representing the constant zero polynomial) is its own successor state and lies on a cycle of length 1. Each of the 63 nonzero states lies on one of three disjoint cycles (of states) of length 21 (see Table 2-1). One cycle corresponds to the 21 elements in Table 1-3 generated by β , a root of

$$f(x) = x^6 + x^5 + x^4 + x^2 + 1$$

The 63 nonzero states correspond to 63 nonzero polynomials over $GF(2)$ which comprise a noncyclic group under polynomial multiplication reduced modulo $f(\beta)$. The remaining two cycles of 21 states correspond to cosets in the group of order 63 relative to the subgroup generated by β . The polynomial

$$\gamma = \beta + 1$$

was arbitrarily selected as one coset leader. Each polynomial in this coset is representable as $\gamma\beta^j$ where $0 \leq j < 21$. The polynomial

$$\delta = \beta^2 + 1$$

serves as the other coset leader in a similar manner. Each element in the latter coset is representable as $\delta\beta^k$ where $0 \leq k < 21$.

Every polynomial over $GF(2)$ is uniquely expressible except for order as the product of powers of irreducible polynomials over $GF(2)$. Irreducible polynomials over any finite are building blocks or atoms as are the primes in the field of integers of infinite order.

$$f(x) = [f_1(x)]^{e_1} \cdot [f_2(x)]^{e_2} \cdot \dots \cdot [f_n(x)]^{e_n}$$

Table 2-1. Equal Length FSR Cycles of (nonzero) States Corresponding to the Decomposition of a Multiplicative Group into a Cyclic Subgroup $\{\beta^i\}$ and Cosets $\{\gamma\beta^j\}$ and $\{\delta\beta^k\}$

i of β^i	$c_5c_4c_3c_2c_1c_0$	j of $\gamma\beta^j$	$c_5c_4c_3c_2c_1c_0$	k of $\delta\beta^k$	$c_5c_4c_3c_2c_1c_0$
0	0 0 0 0 0 1	0	0 0 0 0 1 1	0	0 0 0 1 0 1
1	0 0 0 0 1 0	1	0 0 0 1 1 0	1	0 0 1 0 1 0
2	0 0 0 1 0 0	2	0 0 1 1 0 0	2	0 1 0 1 0 0
3	0 0 1 0 0 0	3	0 1 1 0 0 0	3	1 0 1 0 0 0
4	0 1 0 0 0 0	4	1 1 0 0 0 0	4	1 0 0 1 0 1
5	1 0 0 0 0 0	5	0 1 0 1 0 1	5	1 1 1 1 1 1
6	1 1 0 1 0 1	6	1 0 1 0 1 0	6	0 0 1 0 1 1
7	0 1 1 1 1 1	7	1 0 0 0 0 1	7	0 1 0 1 1 0
8	1 1 1 1 1 0	8	1 1 0 1 1 1	8	1 0 1 1 0 0
9	0 0 1 0 0 1	9	0 1 1 0 1 1	9	1 0 1 1 0 1
10	0 1 0 0 0 1	10	1 1 0 1 1 0	10	1 0 1 1 1 1
11	1 0 0 1 0 0	11	0 1 1 0 0 1	11	1 0 1 0 1 1
12	1 1 1 1 0 1	12	1 1 0 0 1 0	12	1 0 0 0 1 1
13	0 0 1 1 1 1	13	0 1 0 0 0 1	13	1 1 0 0 1 1
14	0 1 1 1 1 0	14	1 0 0 0 1 0	14	0 1 0 0 1 1
15	1 1 1 1 0 0	15	1 1 0 0 0 1	15	1 0 0 1 1 0
16	0 0 1 1 0 1	16	0 1 0 1 1 1	16	1 1 1 0 0 1
17	0 1 1 0 1 0	17	1 0 1 1 1 0	17	0 0 0 1 1 1
18	1 1 0 1 0 0	18	1 0 1 0 0 1	18	0 0 1 1 1 0
19	0 1 1 1 0 1	19	1 0 0 1 1 1	19	0 1 1 1 0 0
20	1 1 1 0 1 0	20	1 1 1 0 1 1	20	1 1 1 0 0 0

where $f_i(x)$ of finite degree is irreducible over GF(2) and the integers $e_i \geq 0$ ($1 \leq i \leq n$). FSR cycles of states associated with reducible polynomials over GF(2) are investigated in the next section.

B. FEEDBACK SHIFT REGISTERS CHARACTERIZED BY RECURRENCE RELATIONS

The behavior of the r -stage shift register with linear-logic feedback, as shown in Figure 2-3, is characterized by the linear recurrence relation

$$a_k = \sum_{i=1}^r c_i a_{k-i}$$

See Reference 3.

Hereafter, FSRs (as shown in Figures 2-1 and 2-2) will be called shift registers with interstage feedback or ISFSRs. Whereas, those shown in Figure 2-3 will be referred to as shift registers with single stage feedback or SSFSRs.

The summation in the linear recurrence relation is to be considered a modulo 2 summation throughout. The content of the i^{th} stage at CPI k is denoted by a_{k-i} . Shifting is implied by the subscripts. The content of the i^{th} stage at CPI k becomes the content of the $(i+1)^{\text{th}}$ stage at CPI $k+1$. That is,

$$a_{k-i} \longrightarrow a_{(k+1)-(i+1)} \quad 1 \leq i < r$$

The c_i 's are Boolean constant multipliers. The i^{th} stage contributes to the feedback if $c_i = 1$. The r^{th} stage is necessarily connected to the feedback (switching) network (i.e., $c_r = 1$). Otherwise, the FSR is using a shift register comprised of less than r stages. The initial state of the

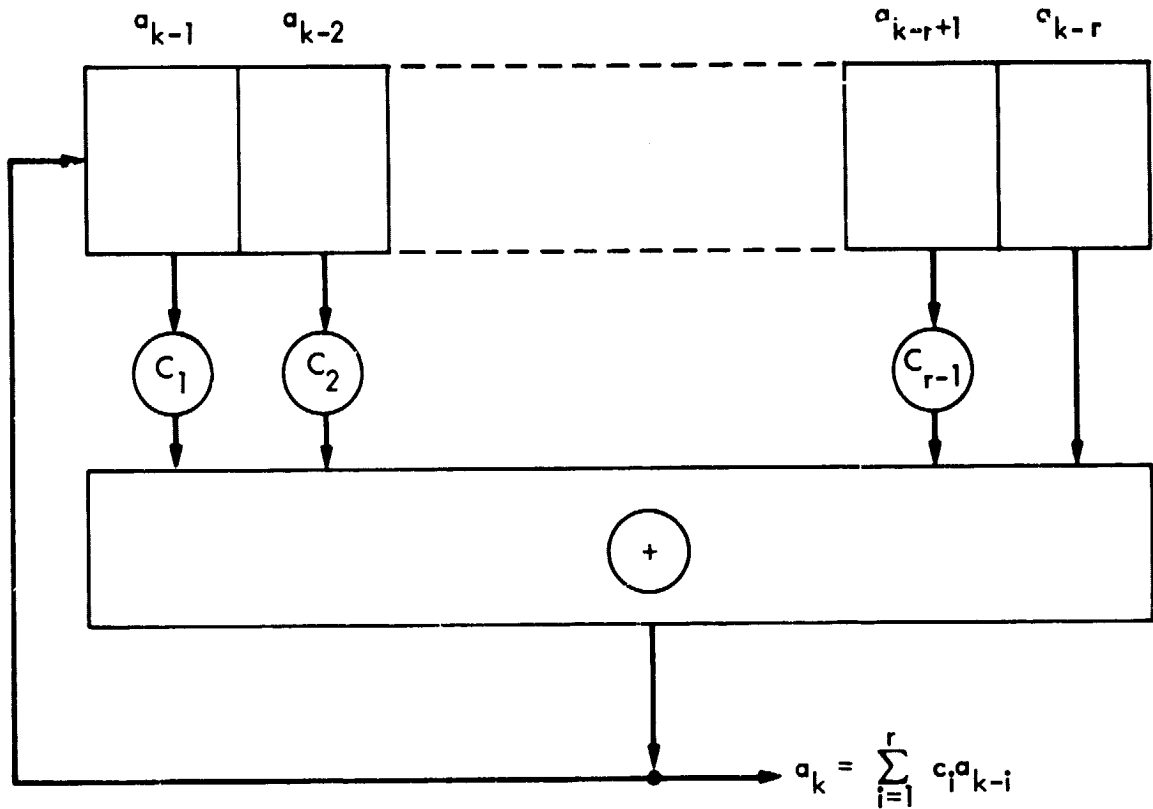


Figure 2-3. Functional Logic Diagram of an r -stage Shift Register with Linear Logic Feedback (SSFSR)

i^{th} stage is denoted by a_{-i} (i.e., a_{k-i} at CPI $k = 0$). The bit being fed back at CPI k is denoted by a_k and a_k becomes the content of the 1^{st} stage at CPI $k + 1$.

$$a_k \rightarrow a_{(k+1)-1}$$

Given

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

a generating function where the sequence of feedback bits are coefficients of ascending powers of x . Then,

$$G(x) = \sum_{i=1}^r c_i x^i \sum_{k=0}^{\infty} a_{k-i} x^{k-i}$$

and

$$G(x) = \sum_{i=1}^r c_i x^i \left[a_{-i} x^{-i} + a_{-i+1} x^{-i+1} + \dots + a_{-1} x^{-1} + \sum_{k=0}^{\infty} a_k x^k \right]$$

Thus,

$$\left(1 - \sum_{i=1}^r c_i x^i \right) G(x) = \sum_{i=1}^r c_i x^i \left[a_{-i} x^{-i} + a_{-i+1} x^{-i+1} + \dots + a_{-1} x^{-1} \right]$$

and

$$G(x) = \frac{g(x)}{f(x)}$$

The numerator

$$g(x) = \sum_{i=1}^r c_i x^i \left[a_{-i} x^{-i} + a_{-i+1} x^{-i+1} + \dots + a_{-1} x^{-1} \right]$$

is of degree less than r and its form is dependent upon the initial state of the FSR ($a_{-1}, a_{-2}, \dots, a_{-r}$) and the feedback connections (c_1, c_2, \dots, c_r). Whereas the denominator

$$f(x) = 1 - \sum_{i=1}^r c_i x^i = 1 + \sum_{i=1}^r c_i x^i$$

(since $-1 \equiv 1 \pmod{2}$) is of degree r (i.e., $c_r = 1$) and its form is dependent upon the feedback connections only. Clearly, $g(x)$ and $f(x)$ are polynomials over $GF(2)$.

The polynomial $f(x)$ is called the characteristic polynomial of the SSFSR. The behavior of the SSFSR can be described by the periodic sequence $\{a_k\}$ corresponding to a given initial state. Overlapping r -bit subsequences of $\{a_k\}$ as seen when $\{a_k\}$ is bit serially passed through an r -bit window, correspond to the state sequence (i.e., cycle of states) assumed by the register portion of the SSFSR.

The period of the longest sequence is governed by the properties of $f(x)$. Given the initial state of the SSFSR in Figure 2-3

$$a_{-1} = a_{-2} = \dots = a_{-r+1} = 0, a_{-r} = 1$$

Then, $g(x) = 1$ and

$$G(x) = \frac{1}{f(x)}$$

Since the SSFSR can only assume a finite number of states before repeating, the sequence

$$\{a_v\} = \{a_0, a_1, \dots, a_{\ell-1}\}$$

must have a finite period $\ell \leq 2^r$. Thus,

$$\begin{aligned} G(x) = \frac{1}{f(x)} &= a_0 + a_1x + \dots + a_{\ell-1}x^{\ell-1} \\ &+ x^\ell (a_0 + a_1x + \dots + a_{\ell-1}x^{\ell-1}) \\ &+ x^{2\ell} (a_0 + a_1x + \dots + a_{\ell-1}x^{\ell-1}) \\ &\vdots \\ &+ x^{m\ell} (a_0 + a_1x + \dots + a_{\ell-1}x^{\ell-1}) \\ &\vdots \\ &= \frac{a_0 + a_1x + \dots + a_{\ell-1}x^{\ell-1}}{1 - x^\ell} \end{aligned}$$

and $f(x)$ divided $1-x^\ell$ for some least integer value ℓ , the periodicity of $\{a_k\}$. Conversely, if $f(x)$ divided $1-x^\ell$ for some least value of ℓ , then $f(x)$ characterizes an SSFSR that generates a periodic sequence of length ℓ when initialized by the state $00, \dots, 01$. Following Reference 3

$$\frac{1-x^\ell}{f(x)} = \gamma_0 + \gamma_1x + \dots + \gamma_{\ell-1}x^{\ell-1}$$

for some least integer value l . Then,

$$\begin{aligned} \frac{1}{f(x)} &= \frac{\gamma_0 + \gamma_1 x + \dots + \gamma_{l-1} x^{l-1}}{1 - x^l} \\ &= (1 + x^l + x^{2l} + \dots + x^{ml} + \dots) (\gamma_0 + \gamma_1 x + \dots + \gamma_{l-1} x^{l-1}) \\ &= G(x) = \sum_{k=0}^{\infty} a_k x^k \end{aligned}$$

Equating coefficients of like powers of x gives $\{\gamma_k\} = \{a_k\}$

Example 8

Given the linear recurrence relation

$$a_k = a_{k-2} + a_{k-3}$$

and the initial conditions $a_{-1} = a_{-2} = 0$ and $a_{-3} = 1$. The linear recurrence relation of order 3 (a discrete analog of a linear differential equation of degree 3 with constant coefficients) with three boundary values (i.e., initial conditions) provides sufficient information to compute a_0, a_1, \dots . The same information can be extracted from $f(x) = 1 + x^2 + x^3$ as follows:

$$\begin{array}{r}
1 + x^2 + x^3 \div \frac{1 + x^2 + x^3 + x^4 + x^7(1 + x^2 + \dots)}{1} \\
\frac{1 + x^2 + x^3}{x^2 + x^3} \\
\frac{x^2}{x^3 + x^4 + x^5} \\
\frac{x^3}{x^4 + x^6} \\
\frac{x^4}{x^7 + \dots}
\end{array}$$

and

$$\{a_k\} = \{1, 0, 1, 1, 1, 0, 0\}$$

The importance of $f(x)$ is that its properties provide information about the periodicity of $\{a_k\}$ without the necessity of determining the components of $\{a_k\}$. Note that $f(x)$ divides $1 - x^7$ and is a primitive polynomial over $GF(2)$ of degree 3.

It will be shown that an r -stage SSFSR and an r -stage ISFSR having identical cycle structures are transformationally equivalent. An isomorphism exists between the states of one and the other.

The generating function of an SSFSR lends itself to readily determining the cycle length for a given initial state, especially when $f(x)$ is reducible. Consider the generating function

$$G(x) = \frac{g(x)}{h(x)s(x)}$$

associated with an r -stage SSFSR whose initial state is nonzero. The characteristic polynomial, $f(x)$, is of degree r and has distinct irreducible factors $h(x)$ and $s(x)$ whose degree exceeds 0. An initial state corresponding to a $g(x)$ that has no common factor (of degree greater than 0) with $f(x)$ lies on a cycle of longest length. That is,

$$(g(x), f(x)) = (g(x), (h(x)s(x))) = 1$$

denoting that the greatest common divisor polynomial is 1, the nonzero constant polynomial. The initial state $0\ 0\ \dots\ 0\ 1$ corresponding to $g(x) = 1$ always lies on a cycle of longest length. By partial fraction expansion

$$G(x) = \frac{1}{h(x)s(x)} = \frac{u(x)}{h(x)} + \frac{v(x)}{s(x)}$$

and

$$u(x)s(x) + v(x)h(x) = 1$$

Unique solutions exist for $u(x)$ and $v(x)$ in the congruential forms

$$u(x)s(x) \equiv 1 \pmod{h(x)}$$

$$v(x)h(x) \equiv 1 \pmod{s(x)}$$

from finite field theory (see Reference 4). Since $u(x)$ is of degree lower than that of $h(x)$ (an irreducible polynomial),

$$(u(x), h(x)) = 1$$

Similarly,

$$((v(x), s(x)) = 1$$

The coefficients of ascending powers of x of the generating function

$$G(x) = \frac{u(x)}{h(x)} + \frac{v(x)}{s(x)}$$

has two components. Its period is the Least Common Multiple (LCM) of the periods of the two components. Thus, if $h(x)$ divides $1 - x^{\ell_1}$, and $s(x)$ divides $1 - x^{\ell_2}$ (for least integer values of ℓ_1 and ℓ_2 , respectively), then

$$f(x) = h(x)s(x) \text{ divides } 1 - x^{\ell}$$

for the least integer value

$$\ell = \text{LCM}(\ell_1, \ell_2)$$

Example 9

Given a seven-stage SSFSR with a characteristic polynomial

$$\begin{aligned} f(x) &= 1 + x + x^3 + x^4 + x^7 \\ &= (1 + x^2 + x^3) (1 + x + x^2 + x^3 + x^4) \end{aligned}$$

Corresponding to the initialization of 0 0 0 0 0 0 1 is the generating function

$$\begin{aligned} G(x) &= \frac{1}{f(x)} = \frac{1}{1 + x + x^3 + x^4 + x^7} \\ &= \frac{1}{(1 + x^2 + x^3) (1 + x + x^2 + x^3 + x^4)} \\ &= \frac{u(x)}{1 + x^2 + x^3} + \frac{v(x)}{1 + x + x^2 + x^3 + x^4} \end{aligned}$$

Thus,

$$u(x) (1 + x + x^2 + x^3 + x^4) + v(x) (1 + x^2 + x^3) = 1$$

and

$$u(x) (x^4 + x^3 + x^2 + x + 1) \equiv 1 \pmod{(x^3 + x^2 + 1)}$$

$$u(x) (x^2 + 1) \equiv 1 \pmod{(x^3 + x^2 + 1)}$$

Also,

$$v(x) (x^3 + x^2 + 1) \equiv 1 \pmod{(x^4 + x^3 + x^2 + x + 1)}$$

The polynomial $u(\alpha)$ is an element in $GF(2^3)$ whose multiplicative generator is α , a root of

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

a primitive polynomial. The multiplicative inverse modulo $x^3 + x^2 + 1$ of

$$(x^2 + 1) \longleftrightarrow (\alpha^2 + 1) \text{ is } u(x) \longleftrightarrow u(\alpha)$$

Since

$$\alpha^7 = 1 \text{ and } \alpha^2 + 1 = \alpha^3$$

$$u(\alpha) = \alpha^4 = \alpha^2 + \alpha + 1$$

and

$$u(x) = 1 + x + x^2$$

The polynomial $v(\beta)$ is an element in $GF(2^4)$. Multiplication of polynomials in the field is reduced modulo

$$s(\beta) = (\beta^4 + \beta^3 + \beta^2 + \beta + 1) \longleftrightarrow (x^4 + x^3 + x^2 + x + 1) = s(x)$$

Since $s(x)$ is a nonprimitive irreducible polynomial, its root β is not a multiplicative generator (of the nonzero elements) in $GF(2^4)$, i.e., $\beta^5 \neq 1$. It may be shown that $\beta + 1$ is one of $\varphi(15) = 8$ multiplicative generators in $GF(2^4)$ where β is a root of

$$s(x) = x^4 + x^3 + x^2 + x + 1$$

as follows:

i of $(\beta + 1)^i$	$c_3c_2c_1c_0$	i of $(\beta + 1)^i$	$c_3c_2c_1c_0$
0	0 0 0 1	8	1 0 0 1
1	0 0 1 1	9	0 1 0 0
2	0 1 0 1	10	1 1 0 0
3	1 1 1 1	11	1 0 1 1
4	1 1 1 0	12	0 0 1 0
5	1 1 0 1	13	0 1 1 0
6	1 0 0 0	14	1 0 1 0
7	0 1 1 1		

The nonzero polynomials in $GF(2^4)$ are expressible as

$$c_3\beta^3 + c_2\beta^2 + c_1\beta^1 + c_0 = (\beta + 1)^i \text{ mod } \beta^4 + \beta^3 + \beta^2 + \beta + 1$$

The multiplicative inverse modulo $x^4 + x^3 + x^2 + x + 1$ of

$$(x^3 + x^2 + 1) \longleftrightarrow \beta^3 + \beta^2 + 1 \text{ is } v(x) \longleftrightarrow v(\beta)$$

Since

$$(\beta + 1)^{15} = 1 \text{ and } \beta^3 + \beta^2 + 1 = (\beta + 1)^5$$

$$v(\beta) = (\beta + 1)^{10} = \beta^3 + \beta^2$$

and

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

A version of Euclid's method which is recursive and detailed in Reference 4 is recommended for determining multiplicative inverses in finite fields of higher order.

The partial fraction expansion is, thus, complete and

$$\begin{aligned} G(x) &= \frac{g(x)}{f(x)} = \frac{1}{1 + x + x^3 + x^4 + x^7} \\ &= \frac{1 + x + x^2}{1 + x^2 + x^3} + \frac{x^2 + x^3}{1 + x + x^2 + x^3 + x^4} \\ &= \frac{u(x)}{h(x)} + \frac{v(x)}{s(x)} \end{aligned}$$

The seven-stage SSFSR may be viewed as being decomposed into a three-stage and a four-stage SSFSR. Its state behavior can be determined from the linear recurrence relation

$$a_k = a_{k-1} + a_{k-3} + a_{k-4} + a_{k-7}$$

with the initial conditions

$$a_{-1} = a_{-2} = \dots = a_{-6} = 0, a_{-7} = 1$$

corresponding to $g(x) = 1$. Successive states $a_{k-1} a_{k-2} \dots a_{k-7}$ and a are tabulated in Table 2-2 for the cycle of states containing the initial state 0 0 , ... , 0 1. Its generating function is

$$G(x) = \frac{1}{1 + x + x^3 + x^4 + x^7}$$

The state behavior of the 3-stage SSFSR is described by

$$b_k = b_{k-2} + b_{k-3}$$

Its generating function, the first term of partial fraction expansion of $G(x)$, is

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

The initial state is determined as follows:

$$\begin{aligned} & b_{-2} + b_{-1}x \\ & + b_{-3} + b_{-2}x + b_{-1}x^2 \\ \hline & = 1 + x + x^2 = u(x) \end{aligned}$$

Thus,

$$\begin{array}{lcl} b_{-1} = 1 & 1 + b_{-2} = 1 & 0 + b_{-3} = 1 \\ & b_{-2} = 0 & b_{-3} = 1 \end{array}$$

Successive states $b_{k-1} b_{k-2} b_{k-3}$ and b_k appear in Table 2-2 for $b_{-1} b_{-2} b_{-3} = 1 0 1$. Since its characteristic polynomial $h(x)$ is of degree 3 and primitive, the periodicity of $\{b_k\}$ is $2^3 - 1$ or 7 and $b_{k-1} = b_{7k-1}$

Table 2-2. State Table of a 7-Stage SSFSR and Components of a Decomposition for

$$f(x) = 1 + x + x^3 + x^4 + x^7 = (1 + x^2 + x^3)(1 + x + x^2 + x^3 + x^4)$$

k	<u>a_{k-1}</u>	<u>a_{k-2}</u>	<u>a_{k-3}</u>	<u>a_{k-4}</u>	<u>a_{k-5}</u>	<u>a_{k-6}</u>	<u>a_{k-7}</u>	a _k	b _{k-1}	<u>b_{k-2}</u>	<u>b_{k-3}</u>	b _k	<u>d_{k-1}</u>	<u>d_{k-2}</u>	<u>d_{k-3}</u>	<u>d_{k-4}</u>	d _k	b _k +d _k = a _k
0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	0	0	1
1	1	0	0	0	0	0	0	1	1	1	0	1	0	1	0	1	0	1
2	1	1	0	0	0	0	0	1	1	1	1	0	0	0	1	0	1	1
3	1	1	1	0	0	0	0	0	0	1	1	0	1	0	0	1	0	0
4	0	1	1	1	0	0	0	0	0	0	1	1	<u>0</u>	<u>1</u>	<u>0</u>	<u>0</u>	<u>1</u>	0
5	0	0	1	1	1	0	0	0	1	0	0	0	1	0	1	0	0	0
6	0	0	0	1	1	1	0	1	<u>0</u>	<u>1</u>	<u>0</u>	<u>1</u>	0	1	0	1	0	1
7	1	0	0	0	1	1	1	0	1	0	1	1	0	0	1	0	1	0
8	0	1	0	0	0	1	1	1	1	1	0	1	1	0	0	1	0	1
9	1	0	1	0	0	0	1	1	1	1	1	0	<u>0</u>	<u>1</u>	<u>0</u>	<u>0</u>	1	1
10	1	1	0	1	0	0	0	0	0	1	1	0	1	0	1	0	0	0
11	0	1	1	0	1	0	0	1	0	0	1	1	0	1	0	1	0	1
12	1	0	1	1	0	1	0	1	0	0	0	0	0	1	0	0	1	1
13	1	1	0	1	1	0	1	1	<u>0</u>	<u>1</u>	<u>0</u>	<u>1</u>	1	0	0	1	0	1
14	1	1	1	0	1	1	0	0	1	0	1	1	<u>0</u>	<u>1</u>	<u>0</u>	<u>0</u>	1	0
15	0	1	1	1	0	1	1	1	1	1	0	1	1	0	1	0	0	1
16	1	0	1	1	1	0	1	0	1	1	1	0	0	1	0	1	0	0
17	0	1	0	1	1	1	0	1	0	1	1	0	0	0	1	0	1	1
18	1	0	1	0	1	1	1	1	0	0	1	1	1	0	0	1	0	1
19	1	1	0	1	0	1	1	1	1	0	0	0	<u>0</u>	<u>1</u>	<u>0</u>	<u>0</u>	<u>1</u>	1
20	1	1	1	0	1	0	1	1	<u>0</u>	<u>1</u>	<u>0</u>	<u>1</u>	1	0	1	0	0	1
21	1	1	1	1	0	1	0	1	1	0	1	1	0	1	1	1	0	1
22	1	1	1	1	1	0	1	0	1	1	0	1	0	0	1	0	1	0
23	0	1	1	1	1	0	0	0	1	1	1	0	1	0	0	1	0	0
24	0	0	1	1	1	1	1	1	0	1	1	0	<u>0</u>	<u>1</u>	<u>0</u>	<u>0</u>	<u>1</u>	1
25	1	0	0	1	1	1	1	1	0	0	1	1	1	0	1	0	0	1
26	1	1	0	0	1	1	1	0	1	0	0	0	0	1	0	1	0	0
27	0	1	1	0	0	1	1	0	<u>0</u>	<u>1</u>	<u>0</u>	<u>1</u>	0	0	1	0	1	0
28	0	0	1	1	0	0	1	1	1	0	1	1	1	0	0	1	0	1
29	1	0	0	1	1	0	0	0	1	1	0	1	<u>0</u>	<u>1</u>	<u>0</u>	<u>0</u>	<u>1</u>	0
30	0	1	0	0	1	1	0	0	1	1	1	0	1	0	1	0	0	0
31	0	0	1	0	0	1	1	0	0	1	1	0	0	1	0	1	0	0
32	0	0	0	1	0	0	1	0	0	0	1	1	0	0	1	0	1	0
33	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	1	0	0
34	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>1</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>1</u>	<u>0</u>	<u>1</u>	<u>0</u>	<u>1</u>	<u>0</u>	<u>0</u>	<u>1</u>	<u>0</u>
0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	0	0	0

The behavior of the 4-stage SSFSR is described by

$$d_k = d_{k-1} + d_{k-2} + d_{k-3} + d_{k-4}$$

Its generating function, the second term of the partial fraction expansion of $G(x)$, is

$$\frac{v(x)}{s(x)} = \frac{x^2 + x^3}{1 + x + x^2 + x^3 + x^4}$$

The feedback connections and the initial state uniquely determines $v(x)$.

$$\begin{aligned} & d_{-1} \\ & + d_{-2} + d_{-1}x \\ & + d_{-3} + d_{-2}x + d_{-1}x^2 \\ & + d_{-4} + d_{-3}x + d_{-2}x^2 + d_{-1}x^3 \\ & = \frac{\quad}{x^2 + x^3} = v(x) \end{aligned}$$

and $d_{-1}d_{-2}d_{-3}d_{-4} = 1010$. Successive states $d_{k-1}d_{k-2}d_{k-3}d_{k-4}$ and d_k appear in Table 2-2 with the foregoing initial state. The characteristic polynomial $s(x)$ is of degree 4. It is a nonprimitive irreducible polynomial whose roots have order 5, a divisor of $2^4 - 1$. Equivalently, $s(x)$ divides $1 - x^{\ell}$ for the least integer value ℓ of 5. The periodicity of $\{d_k\}$ is, thus, 5 and $d_{k-i} = d_{5k-i}$.

As shown in Table 2-2

$$\{a_k\} = \{b_k\} + \{d_k\}$$

and $\{a_k\}$ has period 35, the LCM of 7 (the period of $\{b_k\}$) and 5 (the period of $\{d_k\}$). The LCM of two nonnegative integers a and b is

$$[a, b] = \frac{ab}{(a, b)} \quad a + b > 0$$

Two meshed gears, one with seven teeth (corresponding to the period of $\{b_k\}$) and one with five teeth corresponding to the period of $\{d_k\}$, represent a mechanical analog of the decomposed SSFSRs. A scribe line, joining the centers of the gears before drive is applied to one, corresponds to the initial state. Upon the application of drive, the scribe line of the respective gears rotate (in opposite directions). Both scribe lines will simultaneously first return to their original positions after the number of distinct pairs of teeth that have passed through the point of contact is $[7, 5] = 35$. Equivalently,

$$f(x) = 1 + x + x^3 + x^4 + x^7 \text{ divides } 1 - x^l$$

for the least value of l equal to 35, and the period of $\{a_k\}$ is 35. The order of the roots of $h(x)$, $s(x)$, and $f(x)$ is, respectively

$$\alpha^7 = 1, \beta^5 = 1 \text{ and } \delta^{35} = 1$$

where $h(\alpha) = s(\beta) = f(\delta) = 0$

Given

$$f(x) = \prod_{i=1}^n f_i(x)$$

where each factor $f_i(x)$ is an irreducible polynomial of degree $r_i > 0$ over GF(2) and $f_i(x) \neq f_j(x)$ for $i \neq j$. An irreducible polynomial $f_i(x)$ is said to "belong to exponent l_i ," if $f_i(x)$ divides $1 - x^{l_i}$ but does not divide $1 - x^s$ for $s < l_i$. Also, l_i is the order of α_i where $f_i(\alpha) = 0$.

The "period of $f(x)$ " is

$$= [l_1, l_2, \dots, l_n]$$

the LCM of the exponents to which the distinct irreducible factors belong.

Every irreducible polynomial over GF(2) of degree $r \leq 16$ can be determined from Table C.2 in Appendix C of Reference 6. The table contains a partial list of irreducible polynomials for $16 < r \leq 34$ where factors of $x^{2^r-1} - 1$ belonging to all possible exponents are given. The octal equivalent of the binary coefficient string represents each polynomial. Associated with each polynomial is an integer power (corresponding to an element of a cyclotomic coset) of α , a root of the first entry, a primitive polynomial with a minimum number of terms. Each polynomial listed is the minimal polynomial of the roots corresponding to a cyclotomic coset represented by the element of least value. See Table 1-2 of this report, but note that the primitive polynomial whose root is α (corresponding to 1 in the coset $\{1, 2, 4, 8, 16, 32\}$) differs from the one given in Reference 6. In Reference 6, only one of a pair of reciprocal polynomials is listed. The order of the roots of a listed polynomial (i.e., the exponent to which the polynomial belongs) must be computed as shown in Section I.

Every irreducible polynomial over GF(2) through degree 19 can be determined from Reference 7. As in Reference 6, an octal representation is used for each irreducible polynomial. The octal representations are arranged lexicographically, and the period of each listed polynomial is given. Only the lower-valued octal representation of a reciprocal pair of polynomials is listed. The table enables one to readily determine whether a given polynomial is irreducible.

Reference 8 lists one primitive polynomial over GF(2) with the minimum possible number of terms for every degree through 168. Another list where the numbers of terms is not, in general, a minimum appears in Reference 9 for every degree through 100.

A method of deriving every primitive polynomial of degree r from a given r^{th} degree primitive polynomial appears in Reference 10. Also presented is an outline of an approach to the much more difficult problem of synthesizing a primitive polynomial.

Example 9 is illustrative of the relationship between the period of $f(x)$ and the exponents to which its distinct irreducible factors belong. The period of $f(x)$ corresponds to the period of the longest cycle(s) of states. By initializing the SSFSR with a state corresponding to a $g(x)$ that has a factor in common with $f(x)$, a minor cycle is generated.

Example 10

Consider the 7-stage SSFSR in Example 9. An initial state corresponding to

$$g(x) = s(x) = 1 + x + x^2 + x^3 + x^4$$

results in

$$G(x) = \frac{s(x)}{h(x)s(x)} = \frac{1}{1 + x^2 + x^3}$$

and a sequence $\{a_k\}$ whose period is length 7. From

$$a_k = a_{k-1} + a_{k-3} + a_{k-4} + a_{k-7}$$

$a_{-1} a_{-2}, \dots, a_{-7}$ is determined as follows:

$$\begin{aligned}
 & a_{-1} \\
 & + a_{-3} + a_{-2}x + a_{-1}x^2 \\
 & = a_{-4} + a_{-3}x + a_{-2}x^2 + a_{-1}x^3 \\
 & + a_{-7} + a_{-6}x + a_{-5}x^2 + a_{-4}x^3 + a_{-3}x^4 + a_{-2}x^5 + a_{-1}x^6 \\
 & \hline
 & = 1 + x + x^2 + x^3 + x^4 \\
 & = g(x)
 \end{aligned}$$

$$a_{-1} = a_{-2} = a_{-6} = 0, \quad a_{-3} = a_{-4} = a_{-5} = a_{-7} = 1$$

and the states $a_{k-1} a_{k-2}, \dots, a_{k-7}$ and $\{a_k\}$ versus k are

k	a_{k-1}	a_{k-2}	a_{k-3}	a_{k-4}	a_{k-5}	a_{k-6}	a_{k-7}	a_k
0	0	0	1	1	1	0	1	1
1	1	0	0	1	1	1	0	0
2	0	1	0	0	1	1	1	1
3	1	0	1	0	0	1	1	1
4	1	1	0	1	0	0	1	1
5	1	1	1	0	1	0	0	0
<u>6</u>	<u>0</u>	<u>1</u>	<u>1</u>	<u>1</u>	<u>0</u>	<u>1</u>	<u>0</u>	<u>1</u>
0	0	0	1	1	1	0	1	1

It may be verified that the successive states under any 3 adjacent columns correspond to those generated by a 3-stage SSFSR described by the linear recurrence relationship

$$a_k = a_{k-2} + a_{k-3}$$

and appropriately initialized. In particular, $a_{k-1} a_{k-2} a_{k-3}$ where $a_{-1} a_{-2} a_{-3} = 0 0 1$ mimics the 3-stage SSFSR whose generating function is

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

Refer to Table 2-3. Each of the states in the foregoing length 7 cycle is treated as an initial state and mapped onto its corresponding $g(x)$. Each $g(x)$ is nonzero, of degree 6 or less, and contains

$$s(x) = 1 + x + x^2 + x^3 + x^4$$

as a factor. The remaining factor $\hat{g}(x)$ for each $g(x)$ must be nonzero and of degree 2 or less. There are a total of 7 such $\hat{g}(x)$'s where

$$\hat{g}(x) = c_2 x^2 + c_1 x + c_0$$

and at least one of the three coefficients is nonzero. Each of the 7 states in the length 7 cycle (when used as an initial state) yields

$$G(x) = \frac{\hat{g}(x)}{1 + x^2 + x^3} \quad \text{where} \quad (\hat{g}(x), 1 + x^2 + x^3) = 1$$

It can then be concluded that the 7-stage SSFSR generates one, and only one, cycle of length 7.

An initial state corresponding to

$$g(x) = \hat{g}(x)h(x) = \hat{g}(x)(1 + x^2 + x^3)$$

results in

$$G(x) = \frac{\hat{g}(x)h(x)}{h(x)s(x)} = \frac{\hat{g}(x)}{1 + x + x^2 + x^3 + x^4}$$

Table 2-3. Initial States of a 7-Stage SSFSR that Map onto a $g(x)$ Containing $x^4 + x^3 + x^2 + x + 1$ as a Factor

Initial State							$g(x)$							
a_{-1}	a_{-2}	a_{-3}	a_{-4}	a_{-5}	a_{-6}	a_{-7}	x^6	x^5	x^4	x^3	x^2	x	1	$g(x) = \hat{g}(x)(x^4 + x^3 + x^2 + x + 1)$
0	0	1	1	1	0	1	0	0	1	1	1	1	1	$(\quad)(x^4 + x^3 + x^2 + x + 1)$
1	0	0	1	1	1	0	1	0	0	0	0	1	0	$(x^2 + x)(x^4 + x^3 + x^2 + x + 1)$
0	1	0	0	1	1	1	0	1	0	0	0	0	1	$(x + 1)(x^4 + x^3 + x^2 + x + 1)$
1	0	1	0	0	1	1	1	0	1	1	1	0	1	$(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)$
1	1	0	1	0	0	1	1	1	0	0	0	1	1	$(x^2 + 1)(x^4 + x^3 + x^2 + x + 1)$
1	1	1	0	1	0	0	1	1	1	1	1	0	0	$(x^2)(x^4 + x^3 + x^2 + x + 1)$
0	1	1	1	0	1	0	0	1	1	1	1	1	0	$(x)(x^4 + x^3 + x^2 + x + 1)$
Characteristic Polynomial							$f(x) = (1 + x^2 + x^3)(1 + x + x^2 + x^3 + x^4)$							

Since $g(x)$ is of degree 6 or less, $\hat{g}(x)$ is of degree 3 or less and

$$(\hat{g}(x), x^4 + x^3 + x^2 + x + 1) = 1$$

There are 15 nonzero initial states corresponding to

$$g(x) = (c_3x^3 + c_2x^2 + c_1x + c_0)(x^3 + x^2 + 1)$$

where at least one c_i is nonzero. A simplified approach to determining one initial state is as follows:

k	a_{k-1}	a_{k-2}	a_{k-3}	a_{k-4}	a_{k-5}	a_{k-6}	a_{k-7}	a_k
0	0	0	0	1	-	-	-	1
1	1	0	0	0	1	-	-	1
2	1	1	0	0	0	1	-	0
3	0	1	1	0	0	0	1	0
			\vdots		\vdots			

Embedded in the left four stages is the state-behavior of a 4-stage SSFSR whose generating function is

$$G(x) = \frac{1}{1 + x + x^2 + x^3 + x^4}$$

Furthermore,

$$a_k = a_{k-1} + a_{k-2} + a_{k-3} + a_{k-4}$$

$$a_k = a_{k-1} + a_{k-3} + a_{k-4} + a_{k-7}$$

and

$$0 = a_{k-2} + a_{k-7}$$

$$a_{k-7} = a_{k-2}$$

is sufficient information to fill in the dashed entries.

One cycle of length 7 and 3 cycles of length 5 accounts for 22 states. Each of the states, when viewed as an initial state, maps onto a $g(x)$ where

$$(g(x), f(x)) = x^4 + x^3 + x^2 + x + 1 \text{ or } x^3 + x^2 + 1$$

The all zeros state maps onto $g(x) = 0$ and

$$(0, f(x)) = f(x)$$

corresponds to

$$G(x) = \frac{0}{f(x)} = \frac{0}{1} = 0 = \{a_k\}$$

with periodicity 1. The remaining 105 ($2^8 - 23$) distinct nonzero states when viewed as initial states map onto 105 distinct $g(x)$'s. The greatest

common divisor of each $g(x)$ and

$$f(x) = h(x)s(x) = 1 + x + x^3 + x^4 + x^7$$

is 1. Each of the 105 states is contained in one and only one cycle of length 35. The number of length 35 cycles is 7. The cycle structure of the SSFSR is summarized as follows:

Length of Cycle	Number of Cycle(s)	Number of States
1	1	1
5	3	15
7	1	7
35	7	<u>105</u>
		Total 128

Given that

$$f(x) = [s(x)]^e \quad \text{where the integer } e > 1$$

The length of the longest cycle is the least integer value l for which

$$[s(x)]^e \text{ divides } 1 - x^l$$

The exponent to which $s(x)$ belongs is l_1 and

$$s(x) \text{ divides } 1 - x^{l_1}$$

Also,

$$[s(x)]^e \text{ divides } (1 - x^{\ell_1})^e$$

and

$$(1 - x^{\ell_1})^{2^i} = 1 - x^{2^i \ell_1} \text{ over GF}(2)$$

for integer values $i \geq 0$. The period of $[s(x)]^e$ is thus

$$1 - x^{2^i \ell_1}$$

where $2^{i-1} < e \leq 2^i$

Example 11

Given a 9-stage SSFSR characterized by

$$f(x) = [s(x)]^e = (1 + x^2 + x^3)^3$$

The period of the $s(x)$ is 7.

Since

$$2 < 3 < 2^2$$

$f(x)$ has period $2^2 \cdot 7 = 28$ and the length of the longest cycle that the 9-stage SSFSR can generate is 28. Every state that maps onto a $g(x)$ such that

$$(g(x), [s(x)]^3) = 1$$

is contained in a cycle of length 28. Every state that maps onto a $g(x)$ such that

$$(g(x), [s(x)]^3) = s(x)$$

is contained in a cycle of length $2 \cdot 7 = 14$. Every state that maps onto a $g(x)$ such that

$$(g(x), [s(x)]^3) = [s(x)]^2$$

is contained in a cycle of length 7. The all zeros state maps onto $g(x) = 0$ and

$$(0, [s(x)]^3) = [s(x)]^3$$

Thus, the all zeros state comprises a cycle of length 1.

An SSFSR characterized by

$$f(x) = \prod_{j=1}^n [f_j(x)]^{e_j} \quad e_j \geq 1$$

where $f_j(x)$ has period ℓ_j when initialized with the state $00, \dots, 01$ generates a cycle of longest length

$$\ell = [2^{i_1} \ell_1, 2^{i_2} \ell_2, \dots, 2^{i_n} \ell_n]$$

where $2^{i_j-1} < e_j \leq 2^{i_j}$ and the length of every cycle divides ℓ , the length of the longest cycle.

SECTION III

AN ISOMORPHISM BETWEEN THE STATES OF AN r-STAGE SSFSR AND AN r-STAGE ISFSR

The sequence $\{a_k\}$ emanating from a 4-stage SSFSR satisfies the linear recurrence relation

$$a_k = a_{k-1} + a_{k-2} + a_{k-4} \quad (1)$$

The characteristic polynomial of (1) is

$$f(x) = (1 + x + x^2 + x^4) = (1 + x)(1 + x^2 + x^3) \quad (2)$$

The cycles of states and the corresponding $\{a_k\}$ are tabulated in Table 3-1. Each state in a cycle may be viewed as an initial state that maps onto a $g(x)$. The coefficients of $g(x)$ are linear functions of a_{-1} , a_{-2} , a_{-3} and a_{-4} as follows:

$$\begin{array}{r}
 a_{-1} \\
 + a_{-2} \quad \quad + a_{-1}x \\
 + a_{-4} \quad \quad + a_{-2}x + a_{-2}x^2 + a_{-1}x^3 \\
 \hline
 g(x) = (a_{-1} + a_{-2} + a_{-4}) + (a_{-1} + a_{-3})x + a_{-2}x^2 + a_{-1}x^3 \quad (3)
 \end{array}$$

The coefficients of $g(x)$ are evaluated for each of the 16 states (when viewed as an initial state) on the right side of Table 3-1. It may be noted by inspection that distinct states map onto distinct $g(x)$'s. Thus, a one-to-one correspondence exists between the 16 possible (initial) states and the 16 distinct $g(x)$'s. The states comprise a vector space over GF(2) of dimension 4 (see References 1 and 5). The linearly independent unit vectors form a natural basis and map onto $g(x)$'s in accordance with (3).

Table 3-1. The One-to-One Correspondence Between the States of an SSFSR and the $g(x)$ Polynomials

k	a_{k-1}	a_{k-2}	a_{k-3}	a_{k-4}	a_k	g(x)				
						x^3	x^2	x	1	
0	0	0	0	0	0	x^*	0	0	0	0
0	0	0	0	0	0	x^*	0	0	0	0
0	0	0	0	1	1	1	0	0	0	1
1	1	0	0	0	1	x^6	1	0	1	1
2	1	1	0	0	0	x^5	1	1	1	0
3	0	1	1	0	1	x^4	0	1	1	1
4	1	0	1	1	0	x^3	1	0	0	0
5	0	1	0	1	0	x^2	0	1	0	0
6	0	0	1	0	0	x	0	0	1	0
0	0	0	0	1	1	1	0	0	0	1
0	1	1	1	0	0	γ	1	1	0	0
1	0	1	1	1	0	γx^6	0	1	1	0
2	0	0	1	1	1	γx^5	0	0	1	1
3	1	0	0	1	0	γx^4	1	0	1	0
4	0	1	0	0	1	γx^3	0	1	0	1
5	1	0	1	0	1	γx^2	1	0	0	1
6	1	1	0	1	1	γx	1	1	1	1
0	1	1	1	0	0	γ	1	1	0	0
0	1	1	1	1	1	δ	1	1	0	1
0	1	1	1	1	1	δ	1	1	0	1

$$a_k = a_{k-1} + a_{k-2} + a_{k-4}$$

$$f(x) = x^4 + x^2 + x + 1$$

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

$$x^{-1} = x^6 \equiv x^3 + x + 1 \pmod{f(x)}$$

$$\gamma = x^3 + x^2 = x^2(x + 1)$$

$$\delta = x^3 + x^2 + 1$$

$$\begin{array}{cccc}
 a_{-1} & a_{-2} & a_{-3} & a_{-4} & & x^3 & x^2 & x & 1 \\
 [1 & 0 & 0 & 0] & \longleftrightarrow & [1 & 0 & 1 & 1] \\
 [0 & 1 & 0 & 0] & \longleftrightarrow & [0 & 1 & 0 & 1] \\
 [0 & 0 & 1 & 0] & \longleftrightarrow & [0 & 0 & 1 & 0] \\
 [0 & 0 & 0 & 1] & \longleftrightarrow & [0 & 0 & 0 & 1]
 \end{array}$$

The vectors representing coefficients of corresponding $g(x)$'s are also linearly independent and span a vector space over $GF(2)$ of dimension 4. Two vector spaces of the same dimension and over the same field are isomorphic. The mapping from an SSFSR state to its corresponding ISFSR state is realized by the linear transformation matrix

$$T = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (4)$$

An SSFSR state $a_{k-1}, a_{k-2}, a_{k-3}, a_{k-4}$, which need not be an initial state - i.e., $k \geq 0$, maps onto a ISFSR state as follows:

$$[a_{k-1}, a_{k-2}, a_{k-3}, a_{k-4}]T = [b_3, b_2, b_1, b_0]$$

where $[b_3, b_2, b_1, b_0]$ is the vector representation of

$$b_3x^3 + b_2x^2 + b_1x + b_0 = g(x)$$

Let u and \hat{u} denote any two SSFSR states (not necessarily distinct). Then T in (4) yields

$$(d_1u + d_2\hat{u})T = d_1(uT) + d_2(\hat{u}T)$$

where $c_1, c_2 \in GF(2)$ are scalar multipliers. The inverse of T ,

$$T^{-1} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (5)$$

is the linear transformation matrix that maps every given $g(x)$ to its corresponding SSFSR state. The vectors in T^{-1} in (5) (top to bottom), respectively, represent SSFSR states corresponding to the natural basis $[1, 0, 0, 0]$, $[0, 1, 0, 0]$, $[0, 0, 1, 0]$, and $[0, 0, 0, 1]$, representing x^3 , x^2 , x , and 1.

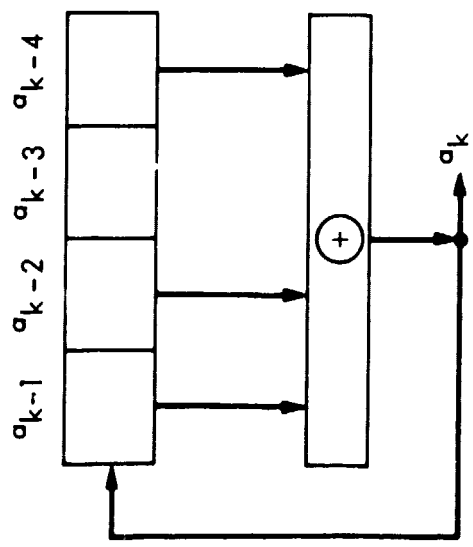
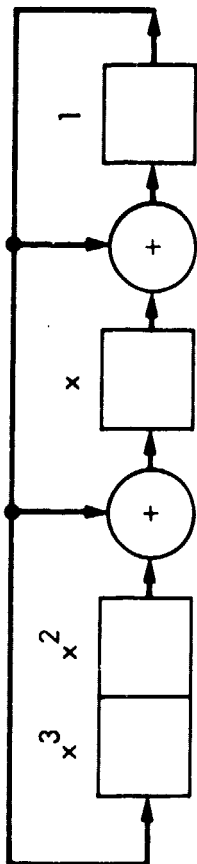
The cycles of $g(x)$'s mathematically describe the behavior of a 4-stage ISFSR that performs division by a root of $f(x)$ in (2). Let α be a root of $f(x)$. Then,

$$\begin{aligned} f(\alpha) = 0 &= 1 + \alpha + \alpha^2 + \alpha^4 \\ 1 &= \alpha^4 + \alpha^2 + \alpha \\ \alpha^{-1} &= \alpha^3 + \alpha + 1 \end{aligned}$$

Note that α has order 7, and $\alpha^{-1} = \alpha^6$ has order 7. The elements α and x are equivalent, i.e., they are the same elements in $GF(2^4)$ with different labels. Thus, $x \longleftrightarrow \alpha$ and

$$x^{-1} = x^6 \equiv x^3 + x + 1 \pmod{x^4 + x^2 + x + 1}$$

The 4-stage ISFSR performs division by x and reduces the result modulo $x^4 + x^2 + x + 1$ (see Figure 3-1).



SSFSR

$$\begin{aligned}
 a_k &= a_{k-1} + a_{k-2} + a_{k-4} \\
 f(x) &= x^4 + x^2 + x + 1 \\
 &= (x + 1)(x^3 + x^2 + 1)
 \end{aligned}$$

ISFSR

REALIZATION OF DIVISION BY
 x MODULO $x^4 + x^2 + x + 1$

Figure 3-1. A 4-Stage SSFSR and a 4-Stage ISFSR with Isomorphic State Spaces

Each of the 16 possible SSFSR states in Table 3-1 maps onto an ISFSR as follows:

$$\begin{bmatrix} a_{k-1} & a_{k-2} & a_{k-3} & a_{k-4} \end{bmatrix} \underbrace{\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}}_T = \begin{bmatrix} a_{k-1} & a_{k-2} & a_{k-1} + a_{k-3} & \\ & a_{k-1} + a_{k-2} + a_{k-4} & & \end{bmatrix} \quad (6)$$

The next SSFSR state (i.e., at CPI $k + 1$) is

$$\begin{bmatrix} a_k & a_{k-1} & a_{k-2} & a_{k-3} \end{bmatrix}$$

where

$$a_k = a_{k-1} + a_{k-2} + a_{k-4}$$

and

$$\begin{bmatrix} a_k & a_{k-1} & a_{k-2} & a_{k-3} \end{bmatrix}^T = \begin{bmatrix} a_k & a_{k-1} & a_k + a_{k-2} & a_k + a_{k-1} + a_{k-3} \end{bmatrix} \quad (7)$$

The right hand side of matrix equations (6) and (7) represent successive transformed SSFSR states appearing in the ISFSR in Figure 3-1 at CPI k and CPI $k + 1$, respectively. Given that the ISFSR stores

$$a_{k-1}, a_{k-2}, a_{k-1} + a_{k-3}, a_k \quad \text{at CPI } k$$

Applying a clock pulse to the ISFSR results in

$$\begin{array}{cccc} 0, & a_{k-1}, & a_{k-2}, & a_{k-1} + a_{k-3} \\ a_k, & 0, & a_k, & a_k \\ \hline a_k, & a_{k-1}, & a_k + a_{k-2}, & a_k + a_{k-1} + a_{k-3} \end{array} \quad (8)$$

The ISFSR state (8) at CPI $k + 1$ is identical to the transformed SSFSR state in (7) at CPI $k + 1$. Thus, the succession of corresponding SSFSR and ISFSR states is preserved under the isomorphism. The next state mappings for the SSFSR and ISFSR are one-to-one onto and described by the following, respective, nonsingular transformation matrices:

$$N_{SS} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad N_{IS} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

The unit vectors comprising the natural basis in an SSFSR vector space do not, in general, belong to the same cycle. However, one cycle in an ISFSR vector space always contains the unit vectors in consecutive positions. The mapping of the unit vectors (in the natural basis) representing SSFSR states is related to $f(x)$ in (2) as follows:

$$f(x) = x^4 + c_3x^3 + c_2x^2 + c_1x + 1$$

$$\text{where } c_3 = 0 \text{ and } c_2 = c_1 = 1$$

$a_{k-1} \ a_{k-2} \ a_{k-3} \ a_k$		$x^3 \ x^2 \ x \ 1$
[1 0 0 0]	→	[1 c_3 c_2 c_1]
[0 1 0 0]	→	[0 1 c_3 c_2]
[0 0 1 0]	→	[0 0 1 c_3]
[0 0 0 1]	→	[0 0 0 1]

The transformation matrix T in (4) is comprised of the foregoing image vectors. The unit vectors (in the natural basis) representing ISFSR states namely, x^3 , x^2 , x , and 1 are in consecutive positions (of a cycle). Their images may be determined directly.

$$x^4 f(1/x) = 1 + x^2 + x^3 + x^4$$

is the reciprocal polynomial of $f(x)$ in (2). It is the characteristic polynomial of the linear recurrence relation

$$b_k = b_{k-2} + b_{k-3} + b_{k-4}$$

that describes the state behavior of a 4-stage SSFSR with the same cycle structure as the SSFSR in Figure 3-1. Corresponding cycles will contain the same states where successive states of one is the reverse of the other for a configuration of the former illustrated as follows.

k	b_{k-4}	b_{k-3}	b_{k-2}	b_{k-1}	a_{k-1}	a_{k-2}	a_{k-3}	a_{k-4}
0	0	0	0	1	0	0	0	1
1	0	0	1	0	1	0	0	0
2	0	1	0	1	1	1	0	0
3	1	0	1	1	0	1	1	0
4	0	1	1	0	1	0	1	1
5	1	1	0	0	0	1	0	1
<u>6</u>	<u>1</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>1</u>	<u>0</u>
0	0	0	0	1	0	0	0	1

Shifting (right to left) as well as labeling ($b_{k-4} b_{k-3} b_{k-2} b_{k-1}$) is the reverse of the SSFSR in Figure 3-1. Since

$$\begin{array}{ccc}
 a_{k-1} a_{k-2} a_{k-3} a_{k-4} & & x^3 \ x^2 \ x \ 1 \\
 [0 \ 0 \ 0 \ 1] & \longleftarrow & [0 \ 0 \ 0 \ 1]
 \end{array}$$

the additional images of interest are those corresponding to the images of three successive predecessors of $x^0 = [0 \ 0 \ 0 \ 1]$, namely x , x^2 , and x^3 .

These are the three successor states of $b_{k-4} b_{k-3} b_{k-2} b_{k-1}$
 $= [0 0 0 1]$ in reverse order. Thus,

$a_{k-1} a_{k-2} a_{k-3} a_{k-4}$	$x^3 \quad x^2 \quad x \quad 1$
[1 0 1 1]	← [1 0 0 0]
[0 1 0 1]	← [0 1 0 0]
[0 0 1 0]	← [0 0 1 0]
[0 0 0 1]	← [0 0 0 1]

The transformation matrix T^{-1} in (5) is comprised of the foregoing image vectors. Note that T in (4) and T^{-1} in (5) are equal for $f(x)$ in (2). However T and T^{-1} are not necessarily equal for other $f(x)$'s.

The significance of the methods presented for determining T and T^{-1} is that they are applicable to every $f(x)$ over $GF(2)$. It obviates the need for generating the corresponding SSFSR and ISFSR cycles which is prohibitive except for small values of r .

The binary sequences in the feedback of the SSFSR and the ISFSR in Figure 3-1 are identical under the isomorphism. That is, a_k equals the coefficient of x^0 for every pair of isomorphic states in Table 3-1.

Self-reciprocal $f(x)$'s characterize FSRs that generate palindromic sequences.

Recall that the generating function

$$G(x) = \frac{g(x)}{f(x)} \tag{9}$$

where

$$g(x) = \sum_{i=1}^r c_i x^i \left[a_{-i} x^{-i} + a_{-i+1} x^{-i+1} + \dots + a_{-1} x^{-1} \right] \quad (9a)$$

$$c_r = 1 \text{ and } f(x) = 1 - \sum_{i=1}^r c_i x^i \quad (9b)$$

characterizes the behavior of an r -stage SSFSR. As previously discussed, each possible SSFSR state may be viewed as an initial state that maps onto a $g(x)$ that represents an isomorphic ISFSR state. If $f(x)$ in (9b) is reducible, an ISFSR state that is a member of a cycle whose length equals the period of a particular irreducible or reducible factor may be determined directly. Furthermore, the length of the cycle to which any given ISFSR state belongs can be readily determined.

Example 12

The SSFSR in Figure 3-1 is characterized by

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

The nonzero ISFSR state belonging to a cycle of length 1 is represented by

$$g(x) = x^3 + x^2 + 1 \text{ or } 1 \ 1 \ 0 \ 1$$

Since

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

is associated with its isomorphic SSFSR state, it is contained on a cycle of length 1 equal to the period of $x + 1$.

CPI	x^3	x^2	x	1
k	1	1	0	1
	0	1	1	0
	<u>1</u>	<u>0</u>	<u>1</u>	<u>1</u>
k + 1	1	1	0	1

and ISFSR state 1 1 0 1 is its own successor.

Example 13

Given an SSFSR described by

$$\begin{aligned}
 f(x) &= x^{10} + x^9 + x^7 + x^5 + x + 1 \\
 &= (x + 1)^3(x^3 + x^2 + 1)(x^4 + x^3 + 1)
 \end{aligned}$$

The period of $(x + 1)^3$ is 4, $x^3 + x^2 + 1$ has period 7, and $x^4 + x^3 + 1$ has period 15. Therefore, the period of $f(x)$ is

$$[4, 7, 15] = 420$$

The ISFSR state 1 1 0 0 1 1 1 0 0 1 corresponding to

$$\begin{aligned}
 g(x) &= x^9 + x^8 + x^5 + x^4 + x^3 + 1 \\
 &= (x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)
 \end{aligned}$$

is contained in a cycle whose length is equal to the period of

$$f(x)/(g(x), f(x))$$

Since

$$(g(x), f(x)) = (x + 1)(x^4 + x^3 + 1)$$

the period of

$$f(x)/((x + 1)(x^4 + x^3 + 1)) = (x + 1)^2(x^3 + x^2 + 1)$$

is $[2, 7]$ or 14. Note that 14 divides 420, the length of the longest cycle(s). The cycle of 14 states is

i of γx^i	$\underline{x^9}$	$\underline{x^8}$	x^7	$\underline{x^6}$	x^5	$\underline{x^4}$	x^3	x^2	x	$\underline{1}$
0	1	1	0	0	1	1	1	0	0	1
419 (-1)	1	0	1	1	0	0	1	1	0	1
418	1	0	0	0	1	1	0	1	1	1
417	1	0	0	1	0	0	1	0	1	0
416	0	1	0	0	1	0	0	1	0	1
415	1	1	1	1	0	0	0	0	1	1
414	1	0	1	0	1	1	0	0	0	0
413	0	1	0	1	0	1	1	0	0	0
412	0	0	1	0	1	0	1	1	0	0
411	0	0	0	1	0	1	0	1	1	0
410	0	0	0	0	1	0	1	0	1	1
409	1	1	0	1	0	0	0	1	0	0
408	0	1	1	0	1	0	0	0	1	0
<u>407 (-13)</u>	<u>0</u>	<u>0</u>	<u>1</u>	<u>1</u>	<u>0</u>	<u>1</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>1</u>
0	1	1	0	0	1	1	1	0	0	1

where

$$x^{-1} = x^{419} \equiv x^9 + x^8 + x^6 + x^4 + 1 \pmod{f(x)}$$

$$\gamma = x^9 + x^8 + x^5 + x^4 + x^3 + 1$$

The SSFSR state isomorphic to the ISFSR state γ (i.e., 1 1 0 0 1 1 1 0 0 1) is

$$\gamma T^{-1} = 1 0 0 1 0 0 0 0 1 1$$

where

$$T^{-1} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

An SSFSR state (vector v) is transformed to its isomorphic ISFSR state by vT where

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

The matrices T and T^{-1} are upper triangular matrices where the elements in the principal diagonal are all 1's. A right shift of the components in each row of T and T^{-1} yield the respective next row of each.

Consider the cycle structure of the SSFSR in Table 3-1. There are a pair of length 1 cycles and a pair of length 7 cycles. The states in one cycle of each pair are the 1's complement of those in the other. From

$$a_k = a_{k-1} + a_{k-2} + a_{k-4}$$

state

$$a_{k-1}, a_{k-2}, a_{k-3}, a_{k-4}$$

is succeeded by

$$a_k, a_{k-1}, a_{k-2}, a_{k-3}$$

Whereas, state $\bar{a}_{k-1}, \bar{a}_{k-2}, \bar{a}_{k-3}, \bar{a}_k$, or

$$1 + a_{k-1}, 1 + a_{k-2}, 1 + a_{k-3}, 1 + a_k$$

is succeeded by $\bar{a}_k, \bar{a}_{k-1}, \bar{a}_{k-2}, \bar{a}_{k-3}$

since

$$(1 + a_{k-1}) + (1 + a_{k-2}) + (1 + a_{k-4}) = 1 + a_k = \bar{a}_k$$

and

$$\begin{aligned} \{a_k\} &= \{1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0\} \\ \{1 + a_k\} &= \{0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1\} \end{aligned}$$

are complementary feedback sequences associated, respectively, with the length 7 complementary cycles of states (see Reference 3).

Consider each pair of corresponding ISFSR cycles of states. The state(s) of one cycle of each pair are of odd weight (i.e., contain an odd number of 1's), whereas the state(s) of the other cycles are of even weight. The sequence of $g(x)$'s, namely, $\{1, x^6, x^5, \dots, x\}$ represent the cycle of ISFSR states which are isomorphic to the cycle of SSFSR states characterized by

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

The elements $\{1, x^6, x^5, \dots, x\}$ form a cyclic group under multiplication. However, they with x^* adjoined do not form a group under vector addition. The vector addition of two distinct vectors of odd weight result in a nonzero vector of even weight. Thus, closure is not satisfied and $\{1, x^6, x^5, \dots, x\}$ with x^* adjoined do not form a field. This is not surprising since $f(x)$ associated with the cycle of nonzero isomorphic states is reducible, hence nonprimitive. The sequence of $g(x)$'s, namely, $\{\gamma, \gamma x^6, \gamma x^5, \dots, \gamma x\}$ where γ equals $x^3 + x^2$ represent the cycle of ISFSR states which are isomorphic to the cycle of SSFSR states characterized by

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

whose denominator $x^3 + x^2 + 1$ is primitive. The elements $\{\gamma, \gamma x^6, \gamma x^5, \gamma x^4, \dots, \gamma x\}$ with x^* adjoined form a field. The multiplicative identity is $x^3 + x^2$ or γ , i.e., $\gamma^2 \equiv \gamma \pmod{f(x)}$

$$(x^3 + x^2)^2 = x^6 + x^4 \equiv x^3 + x^2 \pmod{x^4 + x^2 + x + 1}$$

The multiplicative inverse of γx^j is γx^{7-j} .

$$\begin{aligned} (\gamma x^j)(\gamma x^{7-j}) &= \gamma^2 x^7 \\ &\equiv \gamma \pmod{x^4 + x^2 + x + 1} \end{aligned}$$

The element $x^3 + x^2 + 1$ or δ with x^* adjoined form a field of two elements.

Given the linear recurrence relation

$$a_k = c_0 + \sum_{i=1}^r c_i a_{k-i} \quad (10)$$

where $c_i = 0, 1$ for $0 \leq i < r$ and $c_r = 1$

$$\begin{aligned} G(x) &= \sum_{k=0}^{\infty} a_k x^k = \sum_{k=0}^{\infty} \left(c_0 + \sum_{i=1}^r c_i a_{k-i} \right) x^k \\ &= \sum_{k=0}^{\infty} c_0 x^k + \sum_{i=1}^r c_i x^i \sum_{k=0}^{\infty} a_{k-i} x^{k-i} \end{aligned}$$

The first term expressed in closed form is

$$\frac{c_0}{1-x}$$

The second term can be expressed as

$$g(x) + \left(\sum_{i=1}^r c_i x^i \right) G(x)$$

where $g(x)$ is given in 9(a). It follows that

$$\begin{aligned} G(x) &= \frac{\frac{c_0}{1-x} + g(x)}{f(x)} \\ &= \frac{c_0 + (1-x)g(x)}{(1-x)f(x)} \end{aligned}$$

where $f(x)$ is given in 9(b).

For $c_0 = 0$

$$G(x) = \frac{g(x)}{f(x)}$$

as given in (9).

For $c_0 = 1$

$$G(x) = \frac{1 + (1-x)g(x)}{(1-x)f(x)} = \frac{g_1(x)}{f_1(x)} \quad (11)$$

Since

$$g_1(1) = 1 + (1-1)g(1) = 1.$$

$g_1(x)$ does not contain $x + 1$ as a factor. Hence, $g_1(x)$ has an odd number of terms.

Example 14

$$d_k = 1 + d_{k-2} + d_{k-3}$$

and

$$f_1(x) = (x + 1)(x^3 + x^2 + 1)$$

describe the behavior of the SSFSR in Figure 3-2. The polynomial $g_1(x)$ in (11) versus $d_{-1}d_{-2}d_{-3}$ is derived as follows:

$$g(x) = \frac{\begin{matrix} d_{-2} & + & d_{-1}x \\ + & d_{-3} & + & d_{-2}x + & d_{-1}x^2 \end{matrix}}{d_{-2} + d_{-3} + (d_{-1} + d_{-2})x + d_{-1}x^2}$$

and

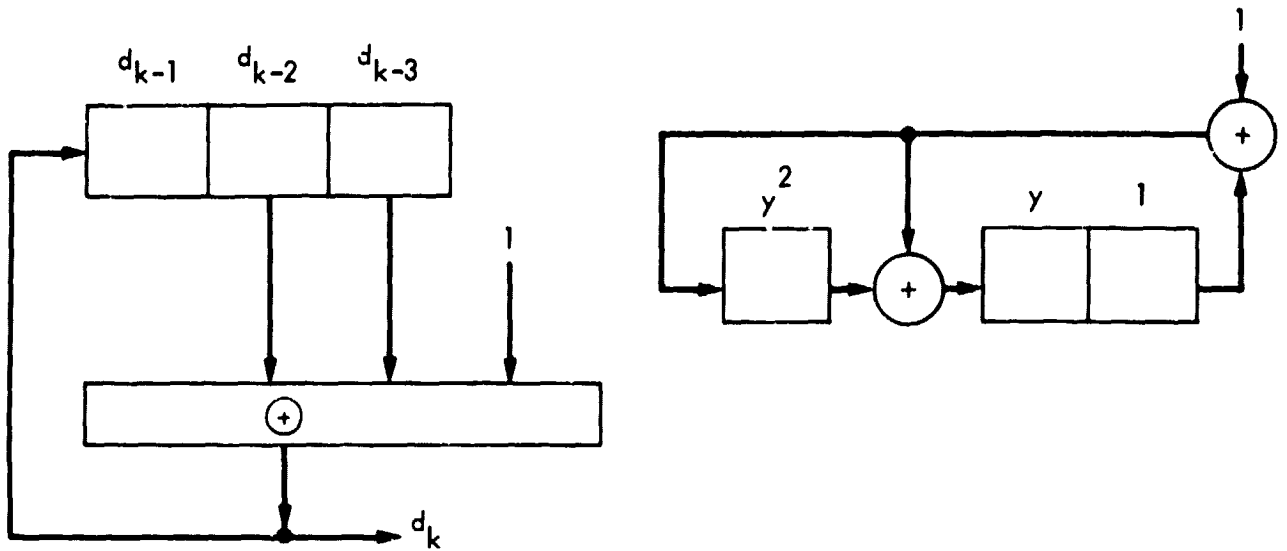
$$g_1(x) = (1 + d_{-2} + d_{-3}) + (d_{-1} + d_{-3})x + d_{-2}x^2 + d_{-1}x^3$$

The successive 3-component SSFSR state vectors map onto the $g_1(x)$ polynomials as shown in Figure 3-2. The two cycles of $g_1(x)$'s of odd weight are respectively identical to the two cycles of $g(x)$'s of odd weight appearing in Table 3-1. Complementation takes place in the feedback path of the SSFSR and the ISFSR in Figure 3-2. A one-to-one correspondence exists between the SSFSR states and ISFSR states. The linear transformation matrix

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

maps $d_{k-1}d_{k-2}d_{k-2}$ into $b_2b_1b_0$ representing $b_2y^2 + b_1y + b_0$. The inverse of T is

$$T^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$



$$d_k = 1 + d_{k-2} + d_{k-3}$$

$$f_1(x) = (1 + x)(1 + x^2 + x^3)$$

$$g_1(x)$$

k	d_{k-1}	d_{k-2}	d_{k-3}	d_k		x^3	x^2	x	1	y^2	y	1
0	0	0	0	1	1	0	0	0	1	0	0	0
1	1	0	0	1	x^6	1	0	1	1	1	1	0
2	1	1	0	0	x^5	1	1	1	0	1	0	1
3	0	1	1	1	x^4	0	1	1	1	0	1	0
4	1	0	1	0	x^3	1	0	0	0	1	1	1
5	0	1	0	0	x^2	0	1	0	0	0	1	1
<u>6</u>	<u>0</u>	<u>0</u>	<u>1</u>	<u>0</u>	<u>x</u>	<u>0</u>	<u>0</u>	<u>1</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>1</u>
0	0	0	0	1	1	0	0	0	1	0	0	0
<u>0</u>	<u>1</u>	<u>1</u>	<u>1</u>	<u>1</u>	<u>δ</u>	<u>1</u>	<u>1</u>	<u>0</u>	<u>1</u>	<u>1</u>	<u>0</u>	<u>0</u>
0	1	1	1	1	δ	1	1	0	1	1	0	0

$$\delta = x^3 + x^2 + 1$$

Figure 3-2. The One-to-One Correspondence Between $d_{k-1}d_{k-2}d_{k-3}$ and $b_2y^2 + b_1y + 1$

Interestingly, T and T^{-1} are the same as those associated with an SSFSR described by

$$a_k = a_{k-2} + a_{k-3}$$

and

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

and an ISFSR that performs division by x modulo $x^3 + x^2 + 1$, i.e., where complementation does not appear in the feedback of the SSFSR or of the ISFSR.

The next state mappings for the SSFSR and the ISFSR in Figure 3-2 are one to one described by affine transformations, a transformation followed by a translation (see Reference 1). Let u denote the present state of the SSFSR and u' the next state. Then

$$u' = uN_{SS} + L_{SS}$$

where

$$N_{SS} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad L_{SS} = [1 \ 0 \ 0]$$

Let v denote the present state of the ISFSR and v' the next state. Then,

$$v' = vN_{IS} + L_{IS}$$

where

$$N_{IS} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad \text{and} \quad L_{IS} = [1 \ 1 \ 0]$$

The binary sequences appearing in the feedback of the SSFSR and ISFSR in Figure 3-2 are identical under the isomorphism. That is, d_k equals $1 + b_0$ (where b_0 is the coefficient of y^0) for every pair of isomorphic states.

Example 15

The behavior of a 4-stage SSFSR is characterized by

$$d_k = 1 + d_{k-1} + d_{k-2} + d_{k-4}$$

and

$$\begin{aligned} f_1(x) &= (1+x)f(x) = (1+x)(1+x+x^2+x^4) \\ &= (1+x)[(1+x)(1+x^2+x^3)] \\ &= (1+x)^2(1+x^2+x^3) \end{aligned}$$

One $1+x$ factor is due to complementation in the feedback, and the generating function is

$$G(x) = \frac{g_1(x)}{f_1(x)} = \frac{1 + (1-x)g(x)}{(1-x)f(x)}$$

Since $g_1(x)$ cannot contain $1-x$ (i.e., $x+1$) as a factor, the SSFSR splits the state space into two cycles. One is of length 14 and contains state 0000. The other is of length 2. For

$$d_{-1} = d_{-2} = d_{-3} = d_{-4} = 0$$

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

The period of $(1 + x)^2$ is 2 and $1 + x^2 + x^3$ has period 7. Thus,

$$l = [2, 7] = 14.$$

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

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

and the state that maps onto $g_1(x) = x^3 + x^2 + 1$ is 0101 (see Table 3-2).

$$g(x) = (d_{-1} + d_{-2} + d_{-4}) + (d_{-1} + d_{-3})x + d_{-2}x^2 + d_{-1}x^3$$

and

$$\begin{aligned} g_1(x) &= 1 + (1 - x)g(x) \\ &= s_0 + s_1x + s_2x^2 + s_3x^3 + s_4x^4 \end{aligned}$$

where

$$\begin{aligned} s_0 &= 1 + d_{-1} + d_{-2} + d_{-4} \\ s_1 &= d_{-2} + d_{-3} + d_{-4} \\ s_2 &= d_{-1} + d_{-2} + d_{-3} \\ s_3 &= d_{-1} + d_{-2} \\ s_4 &= d_{-1} \end{aligned}$$

Since (01) is the only periodic sequence of length 2, it could be deduced that

$$0101 \quad \text{and} \quad 1010$$

Table 3-2. Cycle Structure and Isomorphism of SSFSR and ISFSR States
Whose Respective Next State Transformations are Affine

k	d_{k-1}	d_{k-2}	d_{k-3}	d_{k-4}	d_k	$g_1(x)$				1	$g_2(y)$				
						x^4	x^3	x^2	x		y^3	y^2	y	1	
0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	0
1	1	0	0	0	0	x^{13}	1	1	1	0	0	1	0	1	1
2	0	1	0	0	0	x^{12}	0	1	1	1	0	0	1	0	1
3	0	0	1	0	1	x^{11}	0	0	1	1	1	0	0	1	0
4	1	0	0	1	1	x^{10}	1	1	1	1	1	1	0	1	0
5	1	1	0	0	1	x^9	1	0	0	1	1	1	1	1	0
6	1	1	1	0	1	x^8	1	0	1	0	1	1	1	0	0
7	1	1	1	1	0	x^7	1	0	1	1	0	1	1	0	1
8	0	1	1	1	1	x^6	0	1	0	1	1	0	1	1	0
9	1	0	1	1	1	x^5	1	1	0	0	1	1	0	0	0
10	1	1	0	1	0	x^4	1	0	0	0	0	1	1	1	1
11	0	1	1	0	0	x^3	0	1	0	0	0	0	1	1	1
12	0	0	1	1	0	x^2	0	0	1	0	0	0	0	1	1
13	0	0	0	1	0	x	0	0	0	1	0	0	0	0	1
<hr/>						<hr/>						<hr/>			
0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	0
0	0	1	0	1	1	δ	0	1	1	0	1	0	1	0	0
1	1	0	1	0	0	δx	1	1	0	1	0	1	0	0	1
<hr/>						<hr/>						<hr/>			
0	0	1	0	1	1	δ	0	1	1	0	1	0	1	0	0

$$d_k = 1 + d_{k-1} + d_{k-2} + d_{k-3} + d_{k-4}$$

$$\delta = x^3 + x^2 + 1$$

$$f_1(x) = (1+x)[(1+x)(1+x^2+x^3)]$$

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

are the SSFSR states comprising the cycle of length 2. State 0 1 0 1 maps onto

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

whereas state 1 0 1 0 maps onto

$$g_1(x) = x^4 + x^3 + x = \delta x$$

Refer to Figure 3-2 and Table 3-1. The cycle structure (i.e., two cycles of length 7 and two of length 1) is changed to that of Table 3-2 by incorporating complementation into the feedback paths of the SSFSR and corresponding ISFSR.

Note that

$$T = T^{-1} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

is the same for both sets of isomorphic SSFSR and ISFSR states. The next state mappings, however, are linear and affine transformations, respectively.

An r -stage SSFSR capable of generating $\{a_k\}$ that satisfies the recurrence relation

$$a_k = \sum_{i=1}^r c_i a_{k-i} \quad c_i = 0, 1 \quad \text{for } 1 \leq i < r, \quad c_r = 1 \quad (12)$$

has a characteristic polynomial

$$f(x) = 1 + c_1 x + c_2 x^2 + \cdots + c_{r-1} x^{r-1} + x^r \quad (13)$$

The recurrence relation (12) and $f(x)$ in (13) are implied in the following theorem.

THEOREM 1

Distinct r -stage SSFSR states when viewed as initial states map onto distinct polynomials $g(x)$'s of degree less than r .

Proof

Expanding (9a) gives

$$\begin{aligned}
 g(x) &= c_1 a_{-1} \\
 &+ c_2 (a_{-2} + a_{-1}x) \\
 &\quad \vdots \\
 &+ c_{r-1} (a_{-r+1} + a_{-r+2}x + \dots + a_{-2}x^{r-3} + a_{-1}x^{r-2}) \\
 &+ a_{-r} + a_{-r+1}x + \dots + a_{-3}x^{r-3} + a_{-2}x^{r-2} + a_{-1}x^{r-1} \quad (14)
 \end{aligned}$$

The 2^r state vectors of the SSFSR form a vector space U over $GF(2)$ of dimension r that is spanned by the linearly independent r unit vectors. The mappings of the unit vectors which are a natural basis of the r -dimensional vector space follows from (14).

$$\begin{array}{cccc}
 a_{-1} & a_{-2} & \dots & a_{-r+1} & a_{-r} \\
 [1 & 0 & \dots & 0 & 0] \longrightarrow x^{r-1} + c_{r-1}x^{r-2} + \dots + c_2x + c_1 \\
 [0 & 1 & \dots & 0 & 0] \longrightarrow x^{r-2} + \dots + c_3x + c_2 \\
 & & \vdots & & \vdots \\
 [0 & 0 & \dots & 1 & 0] \longrightarrow x + c_{r-1} \\
 [0 & 0 & \dots & 0 & 1] \longrightarrow 1 \quad (15)
 \end{array}$$

The r images (i.e., $g(x)$'s) are linearly independent polynomials that span a vector space V over $GF(2)$ of dimension r . Thus, each of the 2^r distinct linear combinations maps onto a distinct polynomial $g(x)$ of degree less than r .

Q.E.D.

Each coefficient in

$$b_{r-1}x^{r-1} + b_{r-2}x^{r-2} + \dots + b_0 = g(x)$$

is a distinct linear combination of a_{-1}, a_{-2}, \dots , and a_{-r}

COROLLARY 1.1

The linear transformation

$$T = \begin{matrix} & x^{r-1} & x^{r-2} & x^{r-3} & \dots & x & 1 \\ \begin{bmatrix} 1 & c_{r-1} & c_{r-2} & \dots & c_2 & c_1 \\ 0 & 1 & c_{r-1} & \dots & c_3 & c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & c_{r-1} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix} & & & & & & \end{matrix} \quad (16)$$

is an isomorphism of U onto V .

Proof

The linear transformation matrix T is the one-to-one mapping in (16) where

$$uT = v \quad u \in U \text{ and } v \in V$$

Since the r row vectors of T are linearly independent, T is nonsingular and its inverse T^{-1} exists.

The inverse T^{-1} is a linear transformation. Given (state) vectors v and \hat{v} in V and scalar multipliers e_1 and e_2 in $GF(2)$.

$$\begin{aligned}(e_1 v + e_2 \hat{v})T^{-1}T &= (e_1 v)I + (e_2 \hat{v})I \\ &= [e_1(vT^{-1}) + e_2(\hat{v}T^{-1})]T\end{aligned}$$

Postmultiplying both sides by T^{-1} yields

$$(e_1 v + e_2 \hat{v})T^{-1} = e_1(vT^{-1}) + e_2(\hat{v}T^{-1})$$

thus, T^{-1} is a linear transformation.

The one-to-one onto linear transformation

$$T : U \longrightarrow V$$

is an isomorphism. Every set of linearly independent vectors u_1, u_2, \dots, u_m in U where $m \leq r$ is mapped onto a linearly independent set of vectors v_1, v_2, \dots, v_m in V . When $m = r$, the vector space U is spanned and the vector space V is spanned. For $u_1 = [1, 0, \dots, 0]$, $u_2 = [0, 1, \dots, 0], \dots, u_r = [0, 0, \dots, 1]$, a natural basis for V , every vector $u \in U$ has a unique expression

$$u = a_1 u_1 + a_2 u_2 + \dots + a_r u_r \quad (17)$$

which is a linear combination of the u_i 's. Given that u is expressible as

$$u = h_1 u_1 + h_2 u_2 + \dots + h_r u_r$$

Then,

$$u - u = 0 = (a_{-1} - h_1)u_1 + (a_{-2} - h_2)u_2 + \dots + (a_{-r} - h_r)u_r$$

and since u_1, u_2, \dots, u_r are linearly independent

$$a_{-i} - h_i = 0 \text{ and } h_i = a_{-i} \text{ for all } i.$$

Thus, (17) is unique and uniqueness of representation holds for every given basis.

The respective images of $u_1, u_2, \dots, u_{r-1}, u_r$ are the polynomials in (15) where

$$x^{r-1} + c_{r-1}x^r + \dots + c_2x + c_1$$

is the image of $u_1 = [1, 0, \dots, 0, 0]$. The components of the image vector

$$v_1 = [1, c_{r-1}, \dots, c_2, c_1]$$

are the ordered coefficients of the polynomial $g(x)$ of degree $r-1$ excluding c_0 resulting from the mapping of

$$[a_{-1}, a_{-2}, \dots, a_{-r}] = [1, 0, \dots, 0, 0]$$

in accordance with (15). The vectors v_1, v_2, \dots, v_r are linearly independent and form a basis in V . Postmultiplying both sides of (17) by the transformation matrix T in (16) gives

$$\begin{aligned} uT &= (a_{-1}u_1 + a_{-2}u_2 + \dots + a_{-r}u_r)T \\ &= a_{-1}(u_1T) + a_{-2}(u_2T) + \dots + a_{-r}(u_rT) \end{aligned}$$

Thus,

$$v = a_{-1}v_1 + a_{-2}v_2 + \dots + a_{-r}v_r \quad (18)$$

and every vector $v \in V$ is uniquely expressible relative to the basis v_1, v_2, \dots, v_r .

The a_{-i} 's in (17) and (18) are scalars in the field $GF(2)$. From Reference 1, each basis u_1, u_2, \dots, u_r in a vector space U over a field F provides an isomorphism of U onto space $U_r(F)$. The isomorphism C_u is the correspondence which assigns to each vector $u \in U$ the r -tuple of its coordinates relative to u as follows:

$$(a_{-1}u_1 + a_{-2}u_2 + \dots + a_{-r}u_r)C_u = (a_{-1}, a_{-2}, \dots, a_{-r}) \in U_r(F)$$

where F , in this case, is $GF(2)$. Since the number of vectors r in a basis is determined by the dimension r , which is invariant (as proved in References 1 and 5), every finite-dimensional vector space over a field F is isomorphic to one, and only one, space $U_r(F)$.

Q.E.D.

A more convenient basis in V is

$$\begin{aligned} & [x^{r-1}, 0, \dots, 0, 0] \\ & [0, x^{r-2}, \dots, 0, 0] \\ & \vdots \quad \vdots \quad ; \quad \vdots \quad ; \quad \vdots \quad \vdots \\ & [0, 0, \dots, x, 0] \\ & [0, 0, \dots, 0, 1] \end{aligned}$$

and every element in V may be expressed as

$$b_{r-1}x^{r-1} + b_{r-2}x^{r-2} + \dots + b_1x + b_0 = g(x)$$

From (14),

$$\begin{aligned}
 b_{r-1} &= a_{-1} \\
 b_{r-2} &= c_{r-1}a_{-1} + a_{-2} \\
 &\vdots \quad \quad \quad \vdots \\
 b_1 &= c_2a_{-1} + c_3a_{-2} + \dots + c_{r-1}a_{-r+2} + a_{-r+1} \\
 a_0 = b_0 &= c_1a_{-1} + c_2a_{-2} + \dots + c_{r-2}a_{-r+2} + c_{r-1}a_{-r+1} + a_{-r}
 \end{aligned} \tag{19}$$

Given an r -stage SSFSR capable of generating $\{a_k\}$ that satisfies the linear recurrence relation in (12) and has the characteristic polynomial $f(x)$ given in (13). The state

$$[a_{-1}, a_{-2}, \dots, a_{-r+1}, a_{-r}] = [0, 0, \dots, 0, 1]$$

always has $[1, 0, \dots, 0, 0]$ as its successor state (which may be viewed as another initial state). The corresponding ISFSR states represented as polynomials are

$$\begin{aligned}
 [0, 0, \dots, 0, 1] &\longrightarrow 1 \\
 [1, 0, \dots, 0, 0] &\longrightarrow x^{r-1} + c_{r-1}x^{r-2} + \dots + c_2x + c_1
 \end{aligned}$$

Note that

$$1 \cdot x^{-1} = x^{-1} \equiv (x^{r-1} + c_{r-1}x^{r-2} + \dots + c_2x + c_1) \pmod{f(x)}$$

and 1 divided by x reduced modulo $f(x)$ in (13) is the polynomial representing the ISFSR successor to 1 (the nonzero constant polynomial).

THEOREM 2

Successor states of isomorphic SSFSR and ISFSR states are isomorphic.

Proof

$$[a_{-1}, a_{-2}, \dots, a_{-r+1}, a_{-r}]T = [b_{r-1}, b_{r-2}, \dots, b_1, b_0]$$

where T is given in (16) and each b_i is a distinct linear combination of the a_{-i} 's as shown in (19).

The next state transformation matrix N_{SS} of the r-stage SSFSR is

$$N_{SS} = \begin{bmatrix} c_1 & 1 & 0 & \dots & 0 & 0 \\ c_2 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{r-1} & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \end{bmatrix} \quad (20)$$

The next state transformation matrix N_{IS} of the corresponding r-stage ISFSR is

$$N_{IS} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & c_{r-1} & c_{r-2} & \dots & c_2 & c_1 \end{bmatrix} \quad (21)$$

Denote the successor to

$$u = [a_{-1}, a_{-2}, \dots, a_{-r+1}, a_{-r}]$$

by $u' = [a'_{-1}, a'_{-2}, \dots, a'_{-r+1}, a'_{-r}]$

and the successor to

$$v = [b_{r-1}, b_{r-2}, \dots, b_1, b_0]$$

by $v' = [b'_{r-1}, b'_{r-2}, \dots, b'_1, b'_0]$

Then,

$$\begin{aligned} & [a'_{-1}, a'_{-2}, \dots, a'_{-r+1}, a'_{-r}] \\ &= [a_{-1}, a_{-2}, \dots, a_{-r+1}, a_{-r}]^{N_{SS}} \\ &= [a_0, a_{-1}, \dots, a_{-r+2}, a_{-r+1}] \end{aligned} \tag{22}$$

and

$$\begin{aligned} & [b'_{r-1}, b'_{r-2}, \dots, b'_1, b'_0] \\ &= [b_{r-1}, b_{r-2}, \dots, b_1, b_0]^{N_{IS}} \\ &= [b_0, c_{r-1}b_0 + b_{r-1}, \dots, c_2b_0 + b_2, c_1b_0 + b_1] \end{aligned} \tag{23}$$

where $a_0 = b_0$ is expressed in (19). The assertion that

$$[a'_{-1}, a'_{-2}, \dots, a'_{-r+1}, a'_{-r}]^T = [b'_{r-1}, b'_{r-2}, \dots, b'_1, b'_0]$$

is shown as follows:

In accordance with (19), (22), and (23)

$$\begin{aligned} b'_{r-1} &= a'_{-1} \\ &= a_0 \\ &= \underline{b_0} \end{aligned}$$

$$\begin{aligned} b'_{r-2} &= c_{r-1} a'_{-1} + a'_{-2} \\ &= c_{r-1} a_0 + a_{-1} \\ &= \underline{c_{r-1} b_0 + b_{r-1}} \\ &\vdots \end{aligned}$$

$$\begin{aligned} b'_1 &= c_2 a'_{-1} + (c_3 a'_{-2} + \dots + c_{r-1} a'_{-r+2} + a'_{-r+1}) \\ &= c_2 a_0 + (c_3 a_{-1} + \dots + c_{r-1} a_{-r+1} + a_{-r+2}) \\ &= \underline{c_2 b_0 + b_2} \end{aligned}$$

$$\begin{aligned} b'_0 &= c_1 a'_{-1} + (c_2 a'_{-2} + \dots + c_{r-2} a'_{-r+2} + c_{r-1} a'_{-r+1} + a'_{-r}) \\ &= c_1 a_0 + (c_2 a_{-1} + \dots + c_{r-2} a_{-r+1} + c_{r-1} a_{-r+2} + a_{-r+1}) \\ &= \underline{c_1 b_0 + b_1} \end{aligned}$$

Thus, if

$$uT = v$$

then

$$u'T = v'$$

Furthermore,

$$vT^{-1} = u \text{ and } v'T^{-1} = u'$$

Q.E.D.

It may be concluded from THEOREM 2 that the cycle structure (i.e., the number of cycles of a given length) is identical for an r -stage SSFSR and an r -stage ISFSR with isomorphic state spaces. This is a consequence of the preservation of the next-state operation under the isomorphism

$$T : U \longrightarrow V$$

COROLLARY 2.1

Matrices N_{SS} in (20) and N_{IS} in (21) are similar (see Reference 1).

Proof

$$(uN_{SS})T = u'T = v' = u(N_{SS}T)$$

where T is given in (16).

$$(uT)N_{IS} = vN_{IS} = v' = u(TN_{IS})$$

$N_{SS}T$ and TN_{IS} both map a given $u \in U$ onto the successor of the corresponding $v \in V$, namely v' . Therefore,

$$N_{SS}T = TN_{IS}$$

and

$$N_{SS} = TN_{IS}T^{-1}$$

Q.E.D.

Consider the affine transformation

$$u' = uN_{SS} + L_{SS}$$

where $L_{SS} = [1, 0, \dots, 0]$ a $1 \times r$ vector.

Then,

$$u'T = (uN_{SS})T + L_{SS}T$$

and

$$L_{SS}T = L_{IS} = [1, c_{r-1}, c_{r-2}, \dots, c_2, c_1]$$

From THEOREM 2,

$$(uN_{SS})T = v'$$

prior to the translation by $L_{SS}T$. Given that $u \leftrightarrow v$ and

$$v = [b_{r-1}, b_{r-2}, \dots, b_1, b_0]$$

representing

$$b_{r-1}y^{r-1} + b_{r-2}y^{r-2} + \dots + b_1y + b_0$$

The successor to v , namely vN_{IS} is the vector summation

$$\begin{array}{ccccccc}
 & & y^{r-1} & y^{r-2} & \dots & y & 1 \\
 & & \hline
 & & [0, & b_{r-1}, & \dots, & b_2, & b_1] \\
 & & + b_0[1, & c_{r-1}, & \dots, & c_2, & c_1] \\
 & & \hline
 \end{array}$$

prior to translation by L_{IS} . The vector summation

$$\begin{array}{ccccccc}
 & y^{r-1} & y^{r-2} & \dots & y & 1 & \\
 \hline
 & 0, & b_{r-1}, & \dots, & b_2, & b_1 & \\
 + \bar{b}_0 & [1, & c_{r-1}, & \dots, & c_2, & c_1 &]
 \end{array}$$

(where $\bar{b}_0 = 1 + b_0$) includes the effects of translation by L_{IS} . The content of the rightmost ISFSR stage is b_0 , the scalar multiplier of the feedback vector $[1, c_{r-1}, \dots, c_2, c_1]$. Translation by L_{IS} is realized by complementing b_0 which results in the feedback vector

$$\bar{b}_0 [1, c_{r-1}, \dots, c_2, c_1]$$

The implementation of the ISFSR in Figure 3-2 is an example.

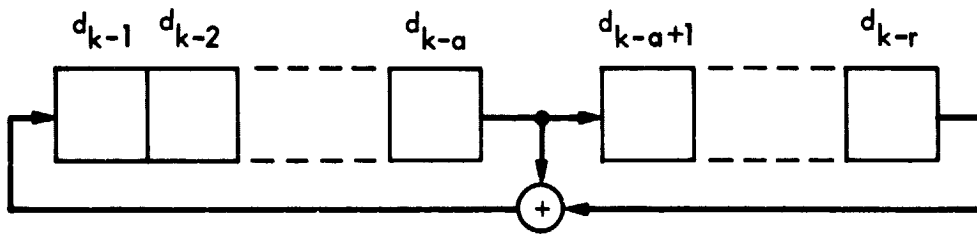
Consider the logical circuitry associated with an SSFSR whose characteristic polynomial

$$f(x) = x^r + x^a + 1$$

is a trinomial. Let α be a root of $f(x)$. Then,

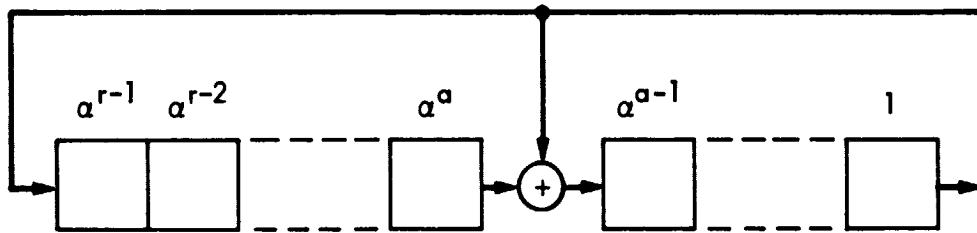
$$\alpha^{-1} = \alpha^{r-1} + \alpha^{a-1}$$

represents the feedback of a corresponding r -stage ISFSR. The ISFSR performs division by α modulo $f(\alpha)$ on its contents. As shown in Figure 3-3, the FSRs are topologically equivalent and of identical complexity (i.e., in the number of switching elements and propagation delay in the feedback).



$$d_k = d_{k-a} + d_{k-r}$$

$$f(x) = x^r + x^a + 1$$



$$f(\alpha) = \alpha^r + \alpha^a + 1 = 0$$

$$\alpha^{-1} \equiv \alpha^{r-1} + \alpha^{a-1} \text{ MODULO } \alpha^r + \alpha^a + 1$$

Figure 3-3. An SSFSR and its Corresponding ISFSR of Identical Complexity

C-2

SECTION IV

THE EXISTENCE AND ALGORITHMIC DETERMINATION OF A TRINOMIAL OF LEAST DEGREE THAT CONTAINS A GIVEN IRREDUCIBLE POLYNOMIAL OVER GF(2) AS A FACTOR

A. PRIMITIVE POLYNOMIALS OVER GF(2)

Primitive polynomials of degree r over GF(2) correspond to r -stage SSFSRs (and ISFSRs) capable of generating PN sequences. A PN sequence satisfies three postulates of randomness as proven in Reference 3.

An example of a binary sequence that is random results from repeated tosses of an ideal coin. Associated with randomness are the following properties:

- (1) The number of heads and tails are approximately equal.
- (2) Short runs of consecutive heads or consecutive tails occur more frequently than long runs. Quantitatively, approximately $1/2$ of the runs are of length 1, $1/4$ of length 2, \dots , $1/2^{i-1}$ of length i , \dots
- (3) The autocorrelation of random sequences is peaked in the middle and sharply drops at the ends.

Consider the periodic binary sequence

$$A_1 = \{a_1, a_2, \dots, a_{l-1}, a_l\} \quad \text{where } l = 2^r - 1$$

emanating from an r -stage SSFSR whose characteristic polynomial is an r th degree primitive polynomial. The randomness postulates satisfied by $\{a_k\}$ are:

P1. Balance

Let w_0 and w_1 denote the number of 0's and 1's, respectively, in $\{a_k\}$. Then,

$$|w_0 - w_1| \leq 1$$

The disparity is exactly 1 for a PN sequence.

P2. Runs and their lengths

Within a period with a_ℓ and a_1 appearing consecutively, there are:

- (1) One run of length r comprised of r consecutive 1's and one run of length $r - 1$ comprised of $r - 1$ consecutive 0's.
- (2) Two runs of length L for each run of length $L+1$ for each value of L where $1 \leq L < r - 1$.

One-half of the runs of length L are comprised of 0's. Runs of 0's alternate with runs of 1's, and the total number of the runs of 0's are equal to the total number of runs of 1's.

P3. Two-valued autocorrelation

The set comprised of

$$\begin{aligned} A_1 &= \{a_1, a_2, \dots, a_{\ell-1}, a_\ell\} \\ A_2 &= \{a_2, a_3, \dots, a_\ell, a_1\} \\ A_3 &= \{a_3, a_4, \dots, a_1, a_2\} \\ &\vdots \\ A_\ell &= \{a_\ell, a_1, \dots, a_{\ell-2}, a_{\ell-1}\} \end{aligned}$$

and

$$A_0 = \{0, 0, \dots, 0, 0\}$$

from an Abelian group G of order 2^r under the binary operation of "addition" defined on G as termwise sum modulo 2.

A_i and A_j satisfy the same linear recurrence relation. Therefore, $A_i + A_j$ for all i and j satisfies the linear recurrence relation. Thus, G is closed under " + " defined on G .

Denote a , b , and c over $GF(2)$ as corresponding terms or components of A_i , A_j , and A_k , respectively. Since

$$(a + b) + c = a + (b + c) \text{ mod } 2$$

elements in G are associative under "+."

The unique identity element of G is A_0 .

$$A_i + A_0 = A_0 + A_i = A_i \text{ for all } i$$

Every element A_i in G has a unique (additive) inverse, namely, itself.

$$A_i + A_i = A_0 \text{ for all } i$$

The elements in G are commutative under "+" since

$$a + b = b + a \text{ mod } 2$$

Thus, G under "+" defined on G is an Abelian group (see References 1, 3, 4, and 5).

The PN sequence and each of its cyclic shifts can be uniquely identified by its first r terms (i.e., components). Each corresponds to a unique initial state of the r -stage SSFSR. Thus, only the first r terms of $A_i + A_j$ need to be determined to identify the resulting sequence.

Again, consider the PN sequence

$$A_1 = \{a_1, a_2, \dots, a_{l-1}, a_l\} \quad \text{where } l = 2^r - 1$$

Let

$$b_i = 1 - 2a_i \text{ for all } i$$

Then, replacing 0's by 1's and 1's by -1's in A_0, A_1, \dots, A_l yields B_0, B_1, \dots, B_l , respectively. The two tables

	a_j	
a_i	0	1
0	0	1
1	1	0

	b_j	
b_i	1	-1
1	1	-1
-1	-1	1

reveal the isomorphism

$$(a_i + a_j) \bmod 2 \longleftrightarrow b_i b_j$$

Thus, $A_i + A_j = A_k$ corresponds to $B_i B_j = B_k$ where the product $B_i B_j$ is taken term-by-term.

The autocorrelation function $C(\tau)$ is two-valued. Explicitly,

$$lC(\tau) = \sum_{k=1}^l b_k b_{k+\tau} = \begin{cases} l & \text{for } \tau = 0 \\ -1 & \text{for } 0 < \tau < l \end{cases}$$

Note that $C(\tau)$ is the dot product of one vector whose components are comprised of 1's and -1's (corresponding to the 0's and 1's of a PN sequence), say B_1 , and B_1 cyclically shifted by τ components. Since $B_i B_j = B_k$ is a vector corresponding to an element in the Abelian group G , it is comprised of l 1's if $i = j$ (i.e., $B_k = B_0$) or one more -1 than 1 if $i \neq j$. Thus, a PN sequence is highly distinguishable from any phase shift of itself.

Example 16

A 31-bit PN sequence is generated by 5-stage SSFSR described by the linear recurrence relation

$$a_k = a_{k-1} + a_{k-2} + a_{k-3} + a_{k-5}$$

whose characteristic polynomial is

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

a primitive polynomial. A period of $\{a_k\}$ appears in Figure 4-1(a).

Of the 31 bits in $\{a_k\}$, 15 are 0's and 16 1's. The postulate P1 on balance is thus satisfied. In general, a PN sequence of period $2^r - 1$ will contain 2^{r-1} 1's and $2^{r-1} - 1$ 0's. The one less 0 is due to the absence of the all zeros state in the cycle of the states of the PN generator.

The run length properties of the PN sequence are shown in Figures 4-1(a) and (b). The distribution of runs is in accordance with postulate P2. In general, a PN sequence of period $2^r - 1$ contains one run of length r and one of length $r-1$. For $1 \leq L < r - 1$, there are 2^{r-1-L} runs of length L , half of which are 0's.

The closure of two distinct elements in $\{B_0, B_1, \dots, B_{\ell}\}$ under termwise multiplication is shown in Figure 4-1(c). In general,

$$a_0 = a_{\ell} \rightarrow b_{\ell} = b_0 \text{ since } \ell \equiv 0 \pmod{2^r - 1}$$

Also,

$$lC(\tau) = \sum_{k=0}^{\ell-1} b_k b_{k+\tau} = \begin{cases} \ell & \text{for } \tau = 0 \\ -1 & \text{for } 0 < \tau < \ell \end{cases}$$

(a)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	1	0	0	1	0	0	1	1	1	1	1	0	1	1	1	0	0	0	1	0	1	0	1	0	1	0	1	0	0	0

(b)

LENGTH L OF RUN	NUMBER N OF RUNS OF LENGTH L	NL
5	1	5
4	1	4
3	2	6
2	4	8
1	8	8
		<hr/>
		31 TOTAL NUMBER OF BITS

(c)

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
b_k	-	+	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+
b_{k+4}	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
$b_k b_{k+4} = b_{k+18}$	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+

Figure 4-1. (a) A 31-bit PN Sequence, (b) its Run Length Properties, (c) Closure Illustrated in the Isomorphic Abelian Group

In normalized form,

$$C(\tau) = \begin{cases} 1 & \text{for } \tau \equiv 0 \pmod{2^r - 1} \\ -\frac{1}{2^r - 1} & \text{for } \tau \not\equiv 0 \pmod{2^r - 1} \end{cases}$$

Specifically, in Figure 4-1(c),

$$31C(4) = -1$$

since

$$b_{k+18} = b_k b_{k+4}$$

is the same sequence as b_k cyclically shifted 18 places to the left. It, thus, has one more -1 than +1 components.

There are four known classes of binary sequences which satisfy both postulates P1 and P3. See Chapter 4 in Reference 11, which terms all sequence in these classes as PN. Of these four classes, only the class of length $2^r - 1$ sequences which can be generated by r -stage SSFSRs or ISFSRs satisfy P2 as well. In this report, only the length $2^r - 1$ sequences are referred to as PN or maximal-length sequences.

Of particular interest are primitive trinomials over $GF(2)$ that characterize PN generators of minimal complexity. However, there are many values of r for which no irreducible r^{th} degree trinomial exists. Furthermore, there are other values of r where irreducible r^{th} degree polynomials exist, but none are primitive. Irreducible trinomials over $GF(2)$ up to degree 1000 were determined by a sequence of four tests in References 12 and 13. The primitive trinomials are distinguished from the irreducible nonprimitive trinomials. The period and/or the index is given for many of the latter.

The only general nontrivial result on trinomials

$$T_{r,k}(x) = x^r + x^k + 1$$

was proven in Reference 14. The parity (even or odd) of the number of factors $T_{r,k}(x)$ is deterministic (from Corollary 5, page 1105 in Reference 14). $T_{r,k}(x)$ has an even number of irreducible factors and, thus, must be factorable if, and only if:

- (1) r is even, k is odd, $r \neq 2k$, and $rk/2 \equiv 0$ or $1 \pmod{4}$
- (2) r is odd, k is even, k does not divide $2r$, and $r \equiv \pm 3 \pmod{8}$
- (3) r is odd, k is even, k divides $2r$, and $r \equiv \pm 1 \pmod{8}$

In all other cases $T_{r,k}(x)$ has an odd number of factors. Note that if r and k are both odd, the reciprocal trinomial $T_{r,r-k}(x)$ is subjected to test (2) or (3).

The foregoing test preceded by two simple tests were used in References 12 and 13 to speedily eliminate reducible trinomials before applying the fourth test (based on an efficient method developed by Berlekamp for factoring polynomials over a finite field). See Chapter 6 in Reference 4.

Example 17

The trinomials $T_{8m,k}(x)$ over $GF(2)$ are reducible. If k is even, $k = 2k_1$, and

$$x^{8m} + x^{2k_1} + 1 = (x^{4m} + x^{k_1} + 1)^2$$

If k is odd,

$$8m \neq 2k \text{ and } 8mk/2 \equiv 0 \pmod{4}$$

Thus, $T_{8m,k}(x)$ has an even number of factors for k odd.

A trinomial $T_{r,k}(x)$ is square-free if, and only if, r and k are not both even. If

$$T_{r,k}(x) = x^r + x^k + 1$$

has a repeated factor, then its derivative

$$T'_{r,k}(x) = (r \bmod 2)x^{r-1} + (k \bmod 2)x^{k-1}$$

is divisible by this factor. Then, $T_{r,k}(x)$ is either: (1) a power of x which is relatively prime to $T_{r,k}(x)$ or (2) is of the form $x^{r-1} + x^{k-1}$. However, a divisor of both

$$x^{r-1} + x^{k-1} \text{ and } x^r + x^k + 1$$

must also be a divisor of

$$x^r + x^k + 1 + x(x^{r-1} + x^{k-1}) = 1$$

Thus, $T_{r,k}(x)$ where r and k are not both even is square-free (see Reference 3). The period of such trinomials is the LCM of the periods of its irreducible factors.

The periods of square-free trinomials over $GF(2)$, their factors, and the periods of their factors through degree 36 are given in Reference 3. Also, the factor of lowest degree is listed for square-free trinomials of degree 37 through 45. The wide applicability of PN sequences has been an impetus in searching for primitive trinomials.

The remainder of this subsection deals with finding trinomials which contain a given primitive polynomial as a factor. The state-behavior of an r -stage PN generator can, thus, be encapsulated by an n -stage SSFSR (or ISFSR) where $n < r$. Additional register stages are the cost of reducing the complexity of the feedback to one 2-input Exclusive-OR gate.

Every nonzero element in $GF(2^r)$ is expressible as an integer power of α .

$$\alpha^j = b_{r-1}\alpha^{r-1} + b_{r-2}\alpha^{r-2} + \dots + b_1\alpha + b_0 \quad (24)$$

where $b_i \in GF(2)$ and α is a root of a primitive polynomial $f(x)$ of degree r over $GF(2)$. Two elements, α^j and α^k , are defined to be a Compatible Pair (CP) if

$$\alpha^j + \alpha^k = 1 \text{ (i.e., } 00 \dots 01) \quad (25)$$

The CP α^j and α^k in (25) correspond to states in an r -stage ISFSR which differ only in b_0 (the content of stage $\alpha^0 = 1$). From (24), the two states are

$$b_{r-1}b_{r-2} \dots b_1b_0 \text{ and } b_{r-1}b_{r-2} \dots b_1\bar{b}_0$$

Lemma 3

Among the $2^r - 1$ nonzero elements in $GF(2^r)$, there are $2^{r-1} - 1$ compatible pairs. Each of the $2^r - 1$ binary r -tuples $(b_{r-1}b_{r-2} \dots b_1b_0)$, except $00 \dots 01$ is compatible with one and only one nonzero r -tuple. The $2^r - 2$ such elements comprise $2^{r-1} - 1$ CPs.

THEOREM 3

Given any r^{th} degree primitive polynomial $f(x)$ over $GF(2)$. Let α be a root of $f(x) = 0$. Then, for every CP α^j and α^k ($k > j$),

$$f(\alpha) \text{ divides } \alpha^k + \alpha^j + 1$$

Thus,

$$f(x) \text{ divides } x^k + x^j + 1$$

Proof

Since α^j and α^k are a CP.

$$\alpha^j + \alpha^k = 1$$

and

$$f(\alpha) = \alpha^k + \alpha^j + 1 = 0$$

Thus, $f(x)$ and $x^k + x^j + 1$ have a common polynomial factor (since they have a common root α in $GF(2^r)$). Since $f(x)$ is irreducible over $GF(2)$,

$$f(x) \text{ divides } x^k + x^j + 1$$

This implies that $k \geq r$ the degree of $f(x)$. Consider the elements (i.e., the polynomials) $1, \alpha, \dots$, and α^{r-1} where α is a root of

$$f(x) = x^r + b_{r-1}x^{r-1} + b_{r-2}x^{r-2} + \dots + b_1x + 1$$

a primitive polynomial over $GF(2)$.

j of α^j	b_{r-1}	b_{r-2}	...	b_1	1
0	0	0	...	0	1
1	0	0	...	1	0
⋮			⋮		
r-2	0	1	...	0	0
r-1	1	0	...	0	0

No CP exists among $1, \alpha, \dots, \alpha^{r-1}$ and

$$\alpha^r = b_{r-1}\alpha^{r-1} + b_{r-2}\alpha^{r-2} + \dots + b_1\alpha + 1$$

is compatible with α^j for one value of $j < r$ if and only if $f(x)$ is a trinomial. If $f(x)$ is not a trinomial, then the degree k of

$$\alpha^k + \alpha^j + 1 = 0$$

exceeds r for all CPs α^j and α^k .

Q.E.D.

COROLLARY 3.1

If α^j and α^k are a CP, then

$$\alpha^{2j \bmod 2^r - 1} \text{ and } \alpha^{2k \bmod 2^r - 1}$$

are a CP in $GF(2^r)$

Proof

If $1 = \alpha^j + \alpha^k$, then

$$1 = (\alpha^j + \alpha^k)^2 = \alpha^{2j \bmod 2^r - 1} + \alpha^{2k \bmod 2^r - 1}$$

Q.E.D.

COROLLARY 3.2

A trinomial of degree $r + 1$ cannot contain an irreducible polynomial, hence, a primitive polynomial of degree r as a factor.

Proof

For a trinomial,

$$T(x) = x^{r+1} + x^j + 1$$

to contain an r^{th} degree irreducible polynomial, it must also have a degree 1 factor. However, since

$$T(0) = 0 + 0 + 1 = 1$$

x is not a factor of $T(x)$, and since

$$T(1) = 1 + 1 + 1 = 1$$

$x + 1$ is not a factor of $T(x)$.

Q.E.D.

The trinomial of least degree (among $2^{r-1} - 1$ trinomials associated with $2^{r-1} - 1$ CPs) that contains a given r^{th} degree primitive polynomial (with five or more odd number of terms) as a factor is of degree $n \geq r + 2$.

Let β be a root of

$$h(x) = x^2 + x + 1$$

Since $h(x)$ divides $x^3 - 1$, β is among the 3 roots of unity. Thus,

$$\beta^3 - 1 = \beta^2 + \beta + 1 = 0$$

and

$$\beta^3 = 1$$

A trinomial

$$T(x) = x^n + x^a + 1$$

is divisible by $h(x)$ if and only if $T(\beta) = 0$. Thus, if

$$\beta^{n \bmod 3} + \beta^{a \bmod 3} + 1 = \beta^2 + \beta + 1$$

$T(x)$ contains $x^2 + x + 1$ as a factor. It is, thus, possible for an r^{th} degree irreducible polynomial to be a factor of a square-free $T(x)$ of degree $n = r + 2$.

Example 18

The trinomial

$$T(x) = x^{16} + x^5 + 1$$

contains $x^2 + x + 1$ as a factor since

$$\beta^{16 \bmod 3} + \beta^{5 \bmod 3} + 1 = \beta^2 + \beta + 1$$

It may be verified that a degree 14 primitive polynomial is the only other factor.

Example 19

The trinomial of least degree that contains the primitive polynomial

$$f(x) = x^6 + x^5 + x^2 + x + 1$$

as a factor is determined algorithmically as follows:

- (1) Initially, $\alpha, \alpha^2, \dots, \alpha^6$, and α^7 are computed and stored as a list of binary state-vectors (see Table 1-1).

i of α^i	b_5	b_4	b_3	b_2	b_1	b_0
1	0	0	0	0	1	0
2	0	0	0	1	0	0
3	0	0	1	0	0	0
4	0	1	0	0	0	0
5	1	0	0	0	0	0
6	1	0	0	1	1	1
7	1	0	1	0	0	1

- (2) α^8 is computed and compared for compatibility with α, α^2, \dots , and α^7 .
- (3) If α^8 is compatible with an element in the initial list, stop. If not, append α^8 to the list and repeat step 2 for a computed α^9 and the augmented list, and so on.

The first CP to be found is α^{11} and α^8 .

i of α^i	b_5	b_4	b_3	b_2	b_1	b_0
1	0	0	0	0	1	0
2	0	0	0	1	0	0
3	0	0	1	0	0	0
4	0	1	0	0	0	0
5	1	0	0	0	0	0
6	1	0	0	1	1	1
7	1	0	1	0	0	1
8	1	1	0	1	0	1
9	0	0	1	1	0	1
10	0	1	1	0	1	0
11	1	1	0	1	0	0
α^{11}	1	1	0	1	0	0
α^8	1	1	0	1	0	1
α^0	0	0	0	0	0	1
$\alpha^{11} + \alpha^8 + 1$	0	0	0	0	0	0

$$f(\alpha) = \alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1 = \alpha^{11} + \alpha^8 + 1 = 0$$

and

$$x^{11} + x + 1 = (x^5 + x^4 + x^3 + x + 1) \underline{(x^6 + x^5 + x^2 + x + 1)}$$

Consider an 11-stage ISFSR that performs multiplication by x and reduces the result modulo $x^{11} + x^8 + 1$. Successive states represent polynomials of degree less than 11 since

$$x^{11} \equiv x^8 + 1 \pmod{x^{11} + x^8 + 1}$$

The cycle in Table 4-1 of length 63 corresponding to the order of α , a root of

$$f(x) = x^6 + x^5 + x^2 + x + 1 = 0$$

contains the state γ representing the factor

$$x^5 + x^4 + x^3 + x + 1 \text{ of } x^{11} + x^8 + 1$$

Recall the isomorphism between SSFSR and ISFSR states where an SSFSR state maps onto $g(x)$ that represents the corresponding ISFSR state. The isomorphism was established using $f(x)$, the characteristic polynomial of the SSFSR and an ISFSR that performs division by x and reduces the result modulo $f(x)$ (see Table 3-1). However, an ISFSR that performs multiplication by x and reduces the result modulo the same $f(x)$ has the same cycle structure with the order of states reversed in each cycle. Thus, $g(x)$'s in a cycle of the former, appear in reverse order in the corresponding cycle of the latter.

The 63-bit PN sequence under column heading b_0 in Table 1-1 is identical to the partially listed sequence under column heading 1 (i.e., x^0) in Table 4-1.

COROLLARY 3.3

The trinomial of least degree that contains a given primitive polynomial $f(x)$ as a factor is square-free.

Proof

Assume

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

is the trinomial of least degree that contains $f(x)$ as a factor. From COROLLARY 3.1, α^n and α^a are compatible and

$$f(x) \text{ divides } x^n + x^a + 1$$

contradicting the assumption.

Q.E.D.

Table 4-1. A 63-State Cycle Associated with
 $x^6 + x^5 + x^2 + x + 1$ a Factor of $x^{11} + x^8 + 1$

i of γx^i	x^{10}	x^9	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x	$\underline{1}$
0	0	0	0	0	0	1	1	1	0	1	1
1	0	0	0	0	1	1	1	0	1	1	0
2	0	0	0	1	1	1	0	1	1	0	0
3	0	0	1	1	1	0	1	1	0	0	0
4	0	1	1	1	0	1	1	0	0	0	0
5	1	1	1	0	1	1	0	0	0	0	0
6	1	1	1	1	1	0	0	0	0	0	1
7	1	1	0	1	0	0	0	0	0	1	1
8	1	0	0	0	0	0	0	0	1	1	1
9	0	0	1	0	0	0	0	1	1	1	1
10	0	1	0	0	0	0	1	1	1	1	0
11	1	0	0	0	0	1	1	1	1	0	0
12	0	0	1	0	1	1	1	1	0	0	1
13	0	1	0	1	1	1	1	0	0	1	0
14	1	0	1	1	1	1	0	0	1	0	0
15	0	1	0	1	1	0	0	1	0	0	1
16	1	0	1	1	0	0	1	0	0	1	0
17	0	1	0	0	0	1	0	0	1	0	1
18	1	0	0	0	1	0	0	1	0	1	0
19	0	0	1	1	0	0	1	0	1	0	1
20	0	1	1	0	0	1	0	1	0	1	0
21	1	1	0	0	1	0	1	0	1	0	0
⋮						⋮					
60	0	1	1	0	1	1	0	0	1	1	1
61	1	1	0	1	1	0	0	1	1	1	0
62	1	0	0	1	0	0	1	1	1	0	1

$$\gamma = x^5 + x^4 + x^3 + x + 1$$

The triomial of least degree that contains a given primitive polynomial over GF(2) as a factor may be determined from Appendix B. One primitive polynomial, $f(x)$, of every reciprocal pair is listed for degrees 5 through 12. The octal equivalent of the binary coefficients in descending powers of x represents $f(x)$. In example 18, it was shown that

$$x^{11} + x^8 + 1 = (x^5 + x^4 + x^3 + x + 1)(\underline{x^6 + x^5 + x^2 + x + 1})$$

The octal representations of the respective factors are 73 and 147. See Appendix B for row entries associated degree r of 6 and $f(x)$ represented by 147. Clearly,

$$x^{11} + x^3 + 1 = (x^5 + x^4 + x^2 + x + 1)(x^6 + x^5 + x^4 + x + 1)$$

The respective octal representations of the factors are 67 and 163. Since 147 and 163 represent a reciprocal pair of primitive polynomials of degree 6, only 147 (with the lower octal representation) and $T(x)$ ($n = 11$, $a = 8$) of lowest degree containing 147 as a factor are listed.

Consider the entries in Appendix B associated with r of 9 (degrees of $f(x)$) and 1243, the octal representation of $f(x)$.

$$T(x) = x^{36} + x + 1 \quad (n = 36, a = 1)$$

The entries under the right-most four columns are as shown as follows:

Irreducible Factors of $T(x)$ in Octal	Degree of Factor	Period	Index
<u>1243</u>	<u>9</u>	<u>511</u>	<u>1</u>
2257*	10	341	3
540663*	17	131071	1

All entries pertaining to $f(x)$ represented as 1243 are in italics. The asterisk (*) appended to the degree 10 factor (2257*) and the degree 17 factor (540663*) indicate that

$$T(x) = x^{36} + x + 1$$

is also the trinomial of least degree that contains each of foregoing factors. The degree 10 factor is nonprimitive and has period 341 (i.e., the order of its roots is 341) and index 3

$$(i.e., (2^{10} - 1)/3 = 341)$$

In terms of Galois Fields, let β be a primitive root n $GF(2^{10})$ of

$$x^{2^{10}-1} - 1 = 0$$

Thus, β^3 has order 341 and is the root of an irreducible nonprimitive degree 10 polynomial whose period is 341 and index is $(3, 2^{10} - 1)$ or 3.

The independent parameters for all entries in Appendix B are r , the degree of $f(x)$, and $f(x)$, the primitive polynomial. The $f(x)$'s of a given degree r are listed in ascending order of n , the degree of the respective $T(x)$ of lowest degree which contains $f(x)$ as a factor. $T(x)$'s of degree $n < 70$ are factored if they are the lowest degree trinomial containing an $f(x)$ of degree 12 or less. Factoring a $T(x)$ (which was determined to be the trinomial of lowest degree containing $f(x)$ of degree r as a factor) often yields irreducible polynomials (primitive and nonprimitive) of degrees greater than r which are not contained in a trinomial of lower degree. The octal representation of these polynomials (as well as those of the same or lower degree than r) are identified by an asterisk (*).

Example 20

The primitive polynomial $f(x)$ of degree 11 represented by 5023 is contained as a factor in

$$T_{47,39}(x) = x^{47} + x^{39} + 1$$

$T_{47,39}(x)$ is the trinomial of least degree that contains 5023 as a factor as determined by the algorithm presented in Example 19. Prior to dividing $T_{47,39}(x)$ by 5023 and factoring the quotient polynomial, it is expedient to extract factors of low degree as follows:

All irreducible factors of degree r are factors of

$$x^{2^r-1} - 1$$

If

$$T_{n,a}(x) = x^n + x^a + 1$$

contains an r^{th} degree factor, then

$$\alpha^{2^r-1} - 1 = \alpha^n + \alpha^a + 1 = 0$$

where α is a root of the r^{th} degree factor. Let $2^r - 1 = w$. Then, $\alpha^w = 1$ and if

$$\alpha^{n \bmod w} + \alpha^{a \bmod w} + 1$$

contains an irreducible r^{th} degree polynomial as a factor, so does $T_{n,a}(x)$. Simplification in extracting factors results only if $w < n$. Specifically,

$$\alpha^{47 \bmod 3} + \alpha^{39 \bmod 3} + 1 = \alpha^2$$

and $T_{47,39}(x)$ does not contain $x^2 + x + 1$ (the only degree 2 irreducible polynomial over $GF(2)$) as a factor.

$$\alpha^{47 \bmod 7} + \alpha^{39 \bmod 7} + 1 = \alpha^5 + \alpha^4 + 1$$

and $\alpha^3 + \alpha + 1$ is a factor of $\alpha^5 + \alpha^4 + 1$. Thus, $x^3 + x + 1$ (13) is a factor of $T_{47,39}(x)$.

$$\alpha^{47 \bmod 15} + \alpha^{39 \bmod 15} + 1 = \alpha^2 + \alpha^9 + 1$$

and $\alpha^4 + \alpha^3 + 1$ is a factor of $\alpha^9 + \alpha^2 + 1$ (see Reference 3). Thus, $x^4 + x^3 + 1$ is a factor of $T_{47,39}(x)$

$$\alpha^{47 \bmod 31} + \alpha^{39 \bmod 31} + 1 = (\alpha^2 + \alpha + 1)^8$$

and $T_{47,39}(x)$ does not contain a degree 5 irreducible polynomial as a factor. Since $w = 2^6 - 1 > 47$, the foregoing test of divisibility cannot be extended beyond irreducible degree 5 factors. Dividing out the irreducible factors 13, 31, and 5023 yields the remaining degree 29 factor $h(x)$ represented by 7036510105. It remains to determine if $h(x)$ is irreducible. Since

$$\alpha^{2^{29}} \equiv \alpha \pmod{h(\alpha)}$$

$h(x)$ is reducible. Repeated squaring

$$\alpha, \alpha^2, \alpha^{2^2}, \dots, \alpha^{2^{29}}$$

where each result is reduced module $h(\alpha)$ is readily realizable on a digital computer.

Squaring any field element in $GF(2^r)$ is equivalent to multiplying the field element (i.e., an r -bit binary vector) by an $r \times r$ binary matrix M . Each term (i.e., power of Q) is squared modulo $h(Q)$. See Chapter 2 of Reference 4 and Example 21.

The aforementioned 29^{th} degree factor is then subjected to Berlekamp's factorization algorithm over $GF(2)$ which is amenable to programming on a digital computer. Applying Berlekamp's factorization algorithm to the 29 degree factor 7036510105 (which is known to be reducible) reveals it has 2 factors. One is 1725 of degree 9 and the other is 4772721 of degree 20. The foregoing results are used to complete the entries in Appendix B which are factors of $T_{47,39}(x)$, the trinomial of least degree that contains $f(x)$ of degree 11 represented by 5023 as a factor. The entries are as follows:

r	Coefficient of $f(x)$ in Octal	$T(x)$ n a	Irreducible Factors of $T(x)$ in Octal	Degree of Factor	Period	Index
<u>11</u>	<u>5023</u>	47 39	13	3	7	1
			31	4	15	1
			1725	9	511	1
			<u>5023</u>	<u>11</u>	<u>2047</u>	<u>1</u>
			4772721*	20	1048575	1

The irreducibility of a factor of degree 19 or less is verified in Reference 7. The test for irreducibility for factors of degree greater than 19 is applied (as illustrated in Example 21). The period of each irreducible factor of degree 19 or less can also be determined from Reference 7. The determination of the period of an irreducible factor of degree $m > 19$ is subsequently discussed.

It remains to ascertain whether each of the factors of $T_{47,39}(x)$ other than 5023 are factors of a trinomial of degree less than $T_{47,39}(x)$. Of the four factors, only 4772721* (as denoted by (*)) of degree 20 is not a factor of a trinomial of degree less than $T_{47,39}(x)$.

Factors 13 and 31 of degrees 3 and 4, respectively, are trinomials, and $T_{45,25}(x)$ is the trinomial of least degree that contains factor 1725 of degree 9.

A 47-stage SSFSR or a 47-stage ISFSR, each with a single 2-input Exclusive-OR gate in the feedback, is characterized by $T_{47,39}(x)$. Properly initialized, the SSFSR and the ISFSR can generate a PN sequence of length 7, 15, 511, 2047, or 1,048,575. Of these, lengths 2047 ($2^{11} - 1$) and 1,048,575 ($2^{20} - 1$) correspond to the most efficient use of the periodic binary sequence generator. Furthermore, a binary sequence whose length is the LCM of any subset of the five available periods could be generated. Initialization is governed by the factors of $T_{47,37}(x)$.

Assume an ISFSR configuration where multiplication (or division) by α , a root of $T_{47,39}(x) = 0$, is performed. To generate a PN sequence of length 1,048,575 ($2^{20} - 1$), a suitable initial state corresponds to the product of the polynomial factors of $T_{47,39}(x)$ excluding 4772721, the primitive polynomial of degree 20. That is,

$$\gamma = (13)(31)(1725)(5023)$$

a polynomial of degree 27 corresponds to a state in the desired cycle.

Example 21

Given the polynomial

$$f(x) = x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$$

Testing whether $f(x)$ is irreducible without resorting to tables may be done as follows:

Any element

$$b_7\alpha^7 + b_6\alpha^6 + \dots + b_1\alpha + b_0$$

represented by $[b_7, b_6, \dots, b_1, b_0]$ may be squared by post multiplication by M over GF(2).

$$M = \begin{matrix} & \alpha^7 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & 1 \\ \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{matrix}$$

where α is a root of $f(x) = 0$. Row 8, 7, ... , 1 in M correspond to polynomials

$$(\alpha^0)^2, (\alpha^1)^2, \dots, (\alpha^7)^2 \pmod{f(\alpha)}$$

respectively. Starting with

$$\alpha = [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0],$$

$$\begin{aligned} \alpha M &= \alpha^2 \\ \alpha^2 M &= \alpha^4 = \alpha^{2^2} \\ &\vdots \\ \alpha^{2^7} M &= \alpha^{256} = \alpha^{2^8} \end{aligned}$$

Reducing each result modulo $f(\alpha)$, yields

	α^7	α^6	α^5	α^4	α^3	α^2	α	1
α^{2^0}	0	0	0	0	0	0	1	0
α^{2^1}	0	0	0	0	0	1	0	0
α^{2^2}	0	0	0	1	0	0	0	0
α^{2^3}	1	0	0	1	1	1	1	1
α^{2^4}	0	1	1	1	1	1	0	1
α^{2^5}	0	1	0	1	1	0	0	1
α^{2^6}	1	0	0	1	0	1	0	0
α^{2^7}	0	0	1	1	1	0	0	0
α^{2^8}	0	0	0	0	0	0	1	0

Since $\alpha^{2^n} \equiv \alpha \pmod{f(\alpha)}$

for a least value of n of 8, the order of α is $2^8 - 1 = 255$ or a divisor of 255. It may be concluded that $f(x)$ is irreducible. However, its period is yet to be determined. ■

An r^{th} degree irreducible $f(x)$ polynomial over $GF(2)$ has period d where d divides $2^r - 1$. Then, unique subsets of

$$\alpha, \alpha^2, \dots, \alpha^{2^{r-1}}$$

reduced modulo $f(x)$ are multiplied to form x^d modulo $f(x)$. The least value of d for which

$$\alpha^d \equiv 1 \pmod{f(\alpha)}$$

is the period of $f(x)$, i.e., the order of its roots. If the least value of d is $2^r - 1$, then $f(x)$ is primitive.

Example 22

In Example 21, it was shown that

$$f(x) = x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$$

is irreducible. The divisors $d > 1$ of 255 are

$$3, 5, 15, 17, 51, 85, 255$$

The number of irreducible polynomials of degree 8 whose roots have order d is $\varphi(d)/8$. Values of 3 and 5 for d can, thus, be ruled out. Clearly,

$$\alpha^d \not\equiv 1 \pmod{f(\alpha)} \text{ for } d = 3, 5.$$

Since

$$\alpha^{16} \not\equiv \alpha \pmod{f(\alpha)}$$

as shown in Example 21, α does not have order 15. Also,

$$\alpha^{17} = \alpha \cdot \alpha^{16} \not\equiv 1 \pmod{f(\alpha)}$$

rules out $d = 17$ which could also be deduced from the fact that $f(x)$ is not a self-reciprocal polynomial. The binary equivalent of 51 is 110011, and

$$\alpha^{51} = \alpha^{16} \alpha^8 \alpha^2 \alpha \equiv 1 \pmod{f(\alpha)}$$

Thus,

$$f(x) = x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$$

has period 51.

Given a primitive polynomial $f(x)$ of degree r over $GF(2)$ comprised of an odd number of terms greater than 3. No method is known of predicting the degree of $T(x)$, a trinomial of lowest degree, which contains $f(x)$ of degree r as a factor. A lower bound was shown to be degree $r + 2$ where

$$T_{r+2,a}(x) = (x^2 + x + 1)f(x)$$

Among

$$\alpha, \alpha^2, \alpha^3, \dots, \alpha^{2^{r-1}}$$

there must be at least one CP. Each of the corresponding 2^{r-1} r -bit vectors has at least one 1 in the first $r - 1$ components. Among these 2^{r-1} $r - 1$ bit segments (where α^* and α^0 are excluded), there must be at least one identical pair. Thus, an upper bound of the degree of $T(x)$ is 2^{r-1} . From entries in Appendix B for $f(x)$'s of degree r from 5 through 12, 2^{r-1} represents a crude upper bound. This is shown tabularly as follows:

r	Coefficient of $f(x)$ in Octal	n	$T(x)$	a	2^{r-1}
5	57	<u>8</u>		3	<u>16</u>
6	147	<u>11</u>		8	<u>32</u>
7	313	<u>21</u>		18	<u>64</u>
8	607	<u>27</u>		8	<u>128</u>
9	163	<u>61</u>		39	<u>256</u>
10	3117	<u>83</u>		14	<u>512</u>
11	5667	<u>143</u>		12	<u>1024</u>
12	1417	<u>171</u>		42	<u>2048</u>

The following statistical model leads to a more reasonable disparity of estimated and actual results. Every r -bit nonzero number appears once, and only once, in an r -stage ISFSR (or SSFSR) cycle characterized by a primitive polynomial of degree r over $GF(2)$. The $2^r - 1$ numbers are, thus, uniformly distributed. Such an ISFSR generates random numbers although a strong dependence exists between a number (i.e., vector state) and its predecessor (see Reference 15).

The statistical model is comprised of cells into which random placing of balls occurs until the first time occurrence of placing a ball into a cell already occupied. The two balls correspond to a Compatible Pair (CP) of ISFSR states. This occupancy model is lucidly presented in Section 7 of Chapter II in Reference 16. Following Feller's approach, (j_1, j_2, \dots, j_n) denotes that the first, second, \dots , and n^{th} ball are placed in cells numbered j_1, j_2, \dots, j_n , and the process terminates on the n^{th} step. The j_i are integers between 1 and $m = 2^r - 1$. For n , only the values 2, 3, \dots , and $m + 1$ are possible. Two balls cannot occupy the same cell before the second step or after the $(m + 1)$ st step.

Attributed to each sample point (j_1, j_2, \dots, j_n) involving exactly n balls is the probability m^{-n} .

The aggregate of all sample points (j_1, j_2, \dots, j_n) for a fixed n corresponds to the event that the process terminates on the n^{th} step.

$$q_n = \frac{P(m, n - 1) \cdot (n - 1)!}{m^n} \quad (26)$$

is the probability a CP is found on the n^{th} step. The permutation of m things taken $n - 1$ at a time is denoted by

$$P(m, n - 1) = m(m - 1) \dots (m - n + 2)$$

The numbered cells j_1, j_2, \dots , and j_{n-1} can be selected in $P(m, n - 1)$ ways. The probability q_n in (26) can be expressed as

$$q_n = \left(1 - \frac{1}{m}\right)\left(1 - \frac{2}{m}\right) \dots \left(1 - \frac{n-2}{m}\right)\left(\frac{n-1}{m}\right) \quad (27)$$

where $q_1 = 0$ and $q_2 = 1/m$

The probability that the process continues for more than n steps is

$$p_n = 1 - (q_1 + q_2 + \dots + q_n)$$

where $p_1 = 1$. By induction,

$$p_n = \frac{P(m, n)}{m^n} = \left(1 - \frac{1}{m}\right)\left(1 - \frac{2}{m}\right) \dots \left(1 - \frac{n-1}{m}\right) \quad (28)$$

For $n \ll m$, cross products can be dropped and

$$p_n \approx 1 - \frac{1 + 2 + \dots + (n-1)}{m} = 1 - \frac{n(n-1)}{2m} \quad (29)$$

Since

$$\text{Ln}(1 - x) \approx -x \quad \text{for small } x > 0$$

where Ln denotes the natural logarithm,

$$\text{Ln } p_n \approx - \frac{1 + 2 + \dots + (n-1)}{m} = - \frac{n(n-1)}{2m}$$

and

$$-\text{Ln } p_n \approx n^2/2m \quad (30)$$

Consider n for which

$$p_1 + p_2 + \dots + p_{n-1} \leq 1/2$$

and

$$p_1 + p_2 + \dots + p_n > 1/2$$

This value of n is the median of the distribution of $\{p_n\}$. The first CP is as likely to be found in n steps as for the process to continue beyond n steps for the first CP to be found. The value of n corresponding to the median of the distribution $\{p_n\}$ is closely approximated by

$$n = (2m \cdot \text{Ln}2)^{0.5} \tag{31}$$

(see Reference 16.) Each primitive polynomial of a given degree r in Appendix B may be considered as corresponding to an experiment. Each represents a different random number generator. The median of the value of n of $\{T_{n,a}(x)\}$ in Appendix B associated with primitive polynomials of a given degree r (5 through 12) is compared with n computed in (31). This is shown tabularly as follows:

r	Median of n in $\{T_{n,a}(x)\}$	$\lceil (2m \cdot \text{Ln}2)^{0.5} \rceil$
5	7	7
6	8	10
7	14	14
8	20	19
9	29	27
10	42	38
11	63	54
12	82	76

Note that $m = 2^r - 1$ and $\lceil x \rceil$ denotes the smallest integer $n \geq x$. The computed value of n corresponding to the median of the distribution $\{p_r\}$ increases with the square root $m = 2^r - 1$. In determining n of $T_{n,a}(x)$ algorithmically, each r -stage ISFSR initially generates the identical ordered set of r r -bit vectors, namely,

$$1, a, a^2, \dots, a^{r-1}$$

and a CP could not appear before step $r + 3$ [or $r + 1$ in the case where $f(x)$ is a trinomial of degree r]. The statistical model does not account for this. Each initialization and succeeding numbers (i.e., vectors) are randomly selected. The low value of n corresponding to the median of the distributions of $\{T_{n,a}(x)\}$ and $\{p_n\}$ compared to the crude upper bound of 2^{r-1} for n is encouraging. Among primitive polynomials of degree $r > 12$, one would expect to find some contained in a $T_{n,a}(x)$ where $n < 10r$. See Appendix B where every $T_{n,a}(x)$ for values of $n < 70$ is factored if it contained a primitive polynomial of degree 12 or less. Irreducible polynomial factors up to degree 55 were found.

A partial list of primitive polynomials from degree 13 through 19 appears in Appendix B. Every (row) entry lists r , the degree of $f(x)$, $f(x)$ of index 1, its reciprocal $x^r f(1/x)$, and the powers of x (n and a) of $T(x)$, the trinomial of lowest degree containing $f(x)$ (or its reciprocal) as a factor. Another factor of $T(x)$ is given if it is an entry that appears elsewhere in Appendix B or Appendix C. If the degree of the second factor is 12 or less, it serves as a cross reference. For example, consider the following row entry:

r	f(x) of Index 1	$x^r f(1/x)$	T(x)		Factor of T(x) Listed Elsewhere			
			n	a	r	Coefficient in Octal	Period	Index
<u>14</u>	70767	<u>73707</u>	<u>53</u>	<u>28</u>	<u>10</u>	<u>2305</u>	<u>1023</u>	<u>1</u>

$T_{53,28}(x)$ was found to be the trinomial of lowest degree to contain the degree 10 polynomial 2305 as a factor. The period of 2305 is 1023 and its index is 1, hence, 2305 is primitive. Among the entries of degree 10 in Appendix B, $f(x)$ represented by 2305 is listed followed by n of 53 and a of 28 associated with $T(x)$, i.e., $T_{53,28}(x)$. The factors of $T_{53,28}(x)$ include the polynomial 73707* of degree 14 whose period is 16,383 and index is 1. The factorization of $T_{53,28}(x)$ led to the primitive degree 14 polynomial 73707*. Note that the degree 14 reciprocal polynomial has a lower octal representation, namely, 70767. However, since 73707 is the factor of $T_{53,28}(x)$, it is italicized in the foregoing example of a listing of a degree 14 primitive polynomial.

There are entries in Appendix B of primitive polynomials of degree 14 through 19 for which no other factor of $T_{n,a}(x)$ is given. Each of the other irreducible factors are either a factor of a trinomial of degree less than n or the degree of each exceeds 19. In the latter cases, the single factor of $T_{n,a}(x)$ was found in the table of factors of square-free trinomials through degree 36 in Reference 3.

In Appendix B (as well as Appendix C), the period (and index) of irreducible factors of $T_{n,a}(x)$ whose degrees exceed 19 were not determined in many cases. These entries are blank.

B. IRREDUCIBLE NONPRIMITIVE POLYNOMIALS OVER GF(2)

Unlike primitive polynomials, there are irreducible nonprimitive polynomials over GF(2) which are not factors of any trinomial. Irreducible nonprimitive polynomials over GF(2) from degree 6 through 12 that are factors of trinomials are listed in Appendix C.

Every irreducible polynomial of degree r over GF(2) where $2^r - 1$ is prime is primitive (see Appendix A). Thus, every irreducible polynomial of degree 2, 3, 5, 7, 13, 17, 19 or 31 are primitive. Primes of the form

$$M_r = 2^r - 1$$

are known as Mersenne primes. A necessary, but not a sufficient condition for M_r to be prime, is that r is prime. See Chapter IX in Reference 3 for a list of 27 of 30 known Mersenne primes.

The Mersenne number (Reference 4)

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$$

is composite through 11 is prime. Of the 186 irreducible polynomials of degree 11, 176 are primitive and 10 are nonprimitive. None of the 10, degree 11 irreducible nonprimitive polynomials (2 of period 23 and 8 of period 89) divide a trinomial.

Given $h(x)$, a degree r irreducible nonprimitive polynomial over $GF(2)$, with an odd number of terms exceeding 3. The subset of elements of $GF(2^r)$ generated by α , a root of $h(x) = 0$, are

$$\alpha, \alpha^2, \dots, \alpha^{d-1}, \alpha^d = 1$$

The order of α is dd where $d < 2^r - 1$ and d divides $2^k - 1$ for $k = r$, but does not divide $2^r - 1$ for $r < k$. Since

$$\alpha^d - 1 = h(\alpha) = 0,$$

the r distinct roots of $h(x) = 0$ are among the d roots of unity. Assume $d = sv$. Then

$$\alpha^v, \alpha^{2v}, \dots, \alpha^{(s-1)v}, \alpha^{sv} = 1$$

are among the d roots of unity. Substituting β for α^v yields

$$\beta, \beta^2, \dots, \beta^{s-1}, \beta^s = 1$$

which comprise the s roots of unity. The s roots of unity are thus a subset of the d roots of unity if s divides d . Furthermore, every element whose

order s divides d must be a power of α , since an element of order s is a generator of the s roots of unity. If the integer s is of the form

$$s = 2^u - 1 > 1$$

then

$$\alpha^v, \alpha^{2v}, \dots, \alpha^{(s-1)v}, \alpha^{sv} = 1$$

are roots of

$$x^{2^u-1} - 1 = 0$$

and are the nonzero elements of $GF(2^u)$. Among the $2^u - 1$ nonzero elements of $GF(2^u)$, there are $2^{u-1} - 1$ Compatible Pairs (CPs). This means that $h(x)$, the irreducible nonprimitive polynomial of degree r , is a factor of a trinomial if the order of a root of $h(x) = 0$, say d , is divisible by s of the form

$$s = 2^u - 1$$

Example 23

The irreducible polynomial

$$h(x) = x^6 + x^5 + x^4 + x^2 + 1,$$

as discussed in Examples 2 and 3, has period 21 (and index 3). Its roots are among the 21 roots of unity. Thus,

$$\beta^{21} - 1 = \beta^6 + \beta^5 + \beta^4 + \beta^2 + 1 = 0$$

and $h(x)$ divides $x^{21} - 1$. The 21 roots of unity are a subset of $GF(2^6)$ and form a group under the defined operation of "multiplication." However,

the 21 roots with 0 (β^*) adjoined do not form a group under the defined operation of "addition." Contained within the 21 roots of unity

$$\beta, \beta^2, \dots, \beta^{20}, \beta^{21} = 1$$

are the nonzero elements of the subfields $GF(2^2)$ and $GF(2^3)$, respectively. Each nonzero element of $GF(2^2)$ is a root of

$$x^{2^2-1} - 1 = x^3 - 1 = 0$$

whereas, each nonzero element of $GF(2^3)$ is a root of

$$x^{2^3-1} - 1 = x^7 - 1 = 0$$

Let $\{\beta^w\}$ be the set of 3 roots of unity.

$$(\beta^w)^3 \text{ mod } 21 = 1 = \beta^0$$

and

$$\begin{aligned} 3w &\equiv 0 \text{ mod } 21 \\ w &\equiv 0 \text{ mod } 21/(3,21) \\ w &\equiv 0 \text{ mod } 7 \\ w &= 0, 7, 14 \end{aligned}$$

Thus,

$$\{\beta^w = \beta^0, \beta^7, \beta^{14}\}$$

are the 3 solutions. From Table 1-3,

$$\beta^7 = 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ \text{ and } \ \beta^{14} = 0 \ 1 \ 1 \ 1 \ 1 \ 0$$

are a CP.

Similarly, let $\{\beta^y\}$ be the set of 7 roots of unity. Then,

$$(\beta^y)^7 \text{ mod } 21 = 1 = \beta^0$$

and

$$\begin{aligned}7y &\equiv 0 \pmod{21} \\ y &\equiv 0 \pmod{21/(7,21)} \\ y &\equiv 0 \pmod{3} \\ y &= 3k \text{ for } k = 0, 1, \dots, 6\end{aligned}$$

Thus,

$$\{\beta^y\} = \{\beta^0, \beta^3, \beta^6, \beta^9, \beta^{12}, \beta^{15}, \beta^{18}\}$$

are the 7 solutions. Placing the nonzero y 's into cyclotomic cosets yields

$$\begin{array}{ccc}3 & 6 & 12 \\ 9 & 18 & 15\end{array}$$

as shown in Table 1-4. Since each coset has an odd number of entries, each member of a CP is associated with a different coset. This is a consequence of Corollary 3.1. It may be verified in Table 1-3 that β^3 and β^9 are a CP. Hence, β^6 and β^{18} as well as β^{12} and β^{15} (due to Corollary 3.1) are CPs.

Applying the algorithm described in Example 19 to

$$h(x) = x^6 + x^5 + x^4 + x^2 + 1$$

in this example reveals that

$$T_{9,3}(x) = x^9 + x^3 + 1$$

is the trinomial of least degree that contains $h(x)$ as a factor. It corresponds to the CP β^3 and β^9 in the subfield $GF(2^3)$. The reciprocal of $h(x)$, namely, $x^6 h(1/x)$ represented by 127 contained in $T_{9,6}(x)$ is an entry in Appendix C.

Example 24

The order of the roots of the degree 12 irreducible nonprimitive polynomial

$$h(x) = x^{12} + x^{10} + x^9 + x^8 + x^7 + x^3 + x^2 + x + 1$$

is 585. The prime factors of 585 are 3^2 , 5, and 13. Since 15 is a divisor of 585, the nonzero elements of $GF(2^4)$ are contained among the 585 roots of unity. Let $\{\beta^w\}$ be the set of 15 roots of unity. Then

$$\begin{aligned} 15w &\equiv 0 \pmod{585} \\ w &\equiv 0 \pmod{585/(15,585)} \\ w &\equiv 0 \pmod{39} \\ w &= 39k \text{ for } k = 0, 1, \dots, 14 \end{aligned}$$

The cyclotomic cosets containing the 14 nonzero values of w are as follows:

39	78	156	312
117	234	468	351
195	390		
273	546	507	429

Dividing each entry by 39 yields

1	2	4	8
3	6	12	9
5	10		
7	14	13	11

which correspond to the 15 roots of unity (excluding $\alpha^0 = 1$) in the isomorphic $GF(2^4)$ generated by a root of $x^4 + x + 1 = 0$ (or a root of its reciprocal $x^4 + x^3 + 1 = 0$). Consider the 7 CPs in the 15 roots of unity generated by α where $\alpha^4 + \alpha + 1 = 0$, the CP α^4 and α correspond to the CP β^{156} , and β^{39} , respectively, and

$$\beta^{156} + \beta^{39} + 1 = h(\beta) = 0,$$

the CP α^4 and α^3 correspond to the CP β^{156} and β^{117} , respectively, and

$$\beta^{156} + \beta^{117} + 1 = \beta^{12} = h(\beta^{12}) = 0.$$

Thus, $h(x)$ is a factor of $T_{156,39}(x)$ and $x^7 h(1/x)$ is a factor of $T_{156,117}(x)$, the reciprocal of $T_{156,39}(x)$. There are

$$\frac{\varphi(585)}{12} = \frac{\varphi(3^2)\varphi(5)\varphi(13)}{12} = 24$$

degree 12 irreducible nonprimitive polynomials over $GF(2)$ of period 585 and index 7. $T_{156,39}(x)$ contains one of each reciprocal pair (12 total) as factors and a degree 12 irreducible nonprimitive polynomial of period 45 (a divisor of 585) and index 91. These are listed as follows:

Irreducible Factors of $T_{156,39}(x)$ in Octal	Degree of Factor	Period	Index
11001	12	45	91
10245	12	585	7
11433	12	585	7
11637 ($h(x)$)	12	585	7
12153	12	585	7
12673	12	585	7
13113	12	585	7
13145	12	585	7
13567	12	585	7
14043	12	585	7
14177	12	585	7
14315	12	585	7
17315	12	585	7

The reciprocal of each of the foregoing degree 12 factors of $T_{156,117}(x)$, the reciprocal of $T_{156,39}(x)$.

Among the 15 roots of unity are β^0 , β^{195} , and β^{390} , the 3 roots of unity. All 24 degree 12 irreducible nonprimitive polynomials whose roots have order 585 are factors of $T_{390,195}(x)$.

Although $T_{156,39}(x)$ is the trinomial of lowest degree derived from the 7 CPs in the 15 roots of unity, it is not the trinomial of lowest degree to contain $h(x)$, whose octal representation is 11637, as a factor. By applying the algorithm illustrated in Example 19, the first CP is found to be β^{11} and β^{23} where

$$\beta^{11} = 1 0 0 0 0 0 0 0 0 0 0 0$$

$$\beta^{23} = 1 0 0 0 0 0 0 0 0 0 0 1$$

Thus,

$$x^{23} + x^{11} + 1 = T_{23,11}(x)$$

is the trinomial of least degree to contain $h(x)$ of degree 12 and period 585 (and index 7) represented by 11637 (see Appendix C). Note that β^{11} and β^{23} among the 585 roots of unity are not members of $GF(2^4)$.

Example 25

The order of the roots of the degree 8 irreducible nonprimitive polynomial

$$h(x) = x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$$

is 85. The prime factors of 85 are 5 and 13, and 85 has no divisors of the form $2^u - 1$. It may be verified that

$$x^{11} + x^5 + 1 = T_{11,5}(x)$$

contains $h(x)$ represented by 567 as a factor, although no subset of 85 roots of unity are the nonzero element of a Galois field. Furthermore, $T_{11,5}(x)$ is the trinomial of least degree containing $h(x)$ as a factor (see Appendix C).

THEOREM 4

A sufficient but not a necessary condition for an irreducible nonprimitive polynomial, $h(x)$, over $GF(2)$ with an odd number of terms exceeding 3 to be a divisor of a trinomial is:

The order of its roots d contains a factor of the form $s = 2^u - 1 > 1$.

Proof

Given $h(x)$ of degree r over $GF(2)$ whose roots have order d where $d < 2^r - 1$ and d divides $2^k - 1$ for $k = r$, but does not divide $2^k - 1$ for $k < r$. Each root of $h(x) = 0$ generates the d roots of unity. If $d = sv$ and

$$s = 2^u - 1 > 1,$$

then, a subset of the d roots of unity is comprised of the nonzero elements of $GF(2^u)$. Each element is a polynomial of degree less than r representable by an r -bit vector. These elements are isomorphic to the nonzero elements in $GF(2^u)$ representable as u -bit vectors. Clearly, u divides r . The $2^u - 1$ u -bit vectors contain $2^{u-1} - 1$ CPs. The isomorphic $2^u - 1$ r -bit vectors also contain $2^{u-1} - 1$ CPs where a compatible pair of r -bit vectors are isomorphic to a compatible pair of u -bit vectors (see Example 6).

The d roots of unity can contain CPs and no subset of elements that comprise a Galois field (see Example 25).

Q.E.D.

COROLLARY 4.1

If β^j and β^k are a CP among the d roots of unity, then

$$\beta^{2j \bmod d} \quad \text{and} \quad \beta^{2k \bmod d}$$

are a CP contained in the d roots of unity.

Proof

$$h(\beta) \mid \beta^k + \beta^j + 1$$

and

$$h(x) \mid x^k + x^j + 1$$

Thus,

$$h(x) \mid (x^k + x^j + 1)^2 = x^{2k} + x^{2j} + 1$$

since

$$[g(x)]^2 = g(x^2)$$

where $g(x)$ is any polynomial over $GF(2)$. Then,

$$\beta^{2k \bmod d} \quad \text{and} \quad \beta^{2j \bmod d}$$

are each members of the d roots of unity

$$\beta, \beta^2, \dots, \beta^{d-1}, \beta^d = 1$$

which form a group under "multiplication" where

$$\beta^w \beta^y = \beta^{(w+y) \bmod d}$$

Since

$$h(x) \mid x^{2k} + x^{2j} + 1$$

$$h(\beta) = \beta^{2k \bmod d} + \beta^{2j \bmod d} + 1 = 0$$

and

$$\beta^{2k \bmod d} \quad \text{and} \quad \beta^{2j \bmod d}$$

are a CP.

Q.E.D.

Example 26

The cyclotomic cosets associated with β^5 and β^{11} , where β is a root of $h(x) = 0$ given in Example 25, respectively, are:

5	10	20	40	80	75	65	45
11	22	44	3	6	12	24	48

The entries in each of the 8 columns are associated with a CP (β^k, β^j) which corresponds to a trinomial divisible by

$$h(x) = x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$$

representable by 567. The square-free trinomials divisible by 567 are listed in ascending order of degree as follows:

$$x^{11} + x^5 + 1$$

$$x^{40} + x^3 + 1$$

$$x^{48} + x^{45} + 1$$

$$x^{65} + x^{24} + 1$$

$$x^{75} + x^{12} + 1$$

The additional square-free trinomials are another source of trinomials of lowest degree that contain an irreducible polynomial of degree greater than 19, e.g., the factors of

$$x^{40} + x^3 + 1$$

are 567 (i.e., $h(x)$ of degree 8 and period 85 and 54556457063, an irreducible polynomial of degree 32. The factors of $2^{32}-1$ are

$$\underbrace{(2^2 - 1)}_3 \underbrace{(2^2 + 1)}_5 \underbrace{(2^4 + 1)}_{17} \underbrace{(2^8 + 1)}_{257} \underbrace{(2^{16} + 1)}_{65,537}$$

and the period of the degree 32 irreducible polynomial divides $2^{32} - 1$. Each of the prime factors may be expressed as

$$F_n = 2^{2^n} + 1$$

for

$$n = 0, 1, 2, 3, 4$$

These are known as Fermat primes. Every F_n Fermat number where $n > 4$, whose character has been determined to date, is composite.

It may be verified that $T_{40,3}(x)$ is the trinomial of least degree that contains the degree 32 irreducible polynomial 54556457063 over GF(2) as a factor.

The following theorem and corollaries are due to Golomb (see Reference 3).

THEOREM 5

A self-reciprocal polynomial over $GF(2)$, $h(x)$, divides a trinomial only if the three roots of unity β^{2a} , β^a , and β^0 for some a are a subset of the elements generated by β , a root of $h(x) = 0$.

Proof

Assume

$$h(x) \mid x^n + x^a + 1$$

Then,

$$x^r h(1/x) \mid x^n + x^{n-a} + 1$$

Given

$$h(x) = x^r h(1/x)$$

Then,

$$h(x) \mid (x^n + x^a + 1) + (x^n + x^{n-a} + 1) = x^{n-a} + x^a$$

Therefore,

$$h(x) \mid x^a(x^{n-a} + x^a) + (x^n + x^a + 1) = x^{2a} + x^a + 1$$

and

$$h(\beta) = \beta^{2a} + \beta^a + 1 = 0$$

The elements β^{2a} and β^a are a CP, and the 3 roots of unity

$$\beta^a, \beta^{2a}, \beta^{3a} = 1$$

are a subset of the elements generated by β . The period of $h(x)$ must, therefore, contain 3 (i.e., $2^2 - 1$) as a factor.

Q.E.D. .

COROLLARY 5.1

No trinomial is divisible by both $x^3 + x + 1$ and $x^3 + x^2 + 1$.

Proof

$$u(x) = (x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

a self-reciprocal polynomial whose roots have order 7, and 7 is not divisible by 3.

The elements generated by β , a root of $u(x) = 0$ are

i of β^i	c_5	c_4	c_3	c_2	c_1	c_0
0	0	0	0	0	0	1
1	0	0	0	0	1	0
2	0	0	0	1	0	0
3	0	0	1	0	0	0
4	0	1	0	0	0	0
5	1	0	0	0	0	0
6	1	1	1	1	1	1
—	—————					
0	0	0	0	0	0	1

and no CP is among them.

Q.E.D.

COROLLARY 5.2

No trinomial is divisible by

$$h(x) = x^4 + x^3 + x^2 + x + 1$$

an irreducible self-reciprocal polynomial whose roots have order 5.

Proof

Since 3 is not a divisor of 5,

$$x^3 - 1 \text{ does not divide } x^5 - 1$$

and all 3 roots of unity are not a subset of the 5 roots of unity.

The 5 roots of unity generated by β , a root of $h(x) = 0$, do not contain a CP.

Q.E.D.

Example 27

There are 6 self-reciprocal irreducible polynomials of degree 18 whose roots have order 171 (and index 1533). See Table 1-5.

Let $\{\beta^a\}$ be the set of 3 roots of unity which are a subset of the 171 roots of unity.

$$(\beta^a)^3 \text{ mod } 171 = 1 = \beta^0$$

and

$$\begin{aligned} 3a &\equiv 0 \text{ mod } 171 \\ a &\equiv 0 \text{ mod } 171/(171/3) \\ a &\equiv 0 \text{ mod } 54 \\ a &= 0, 57, 114 \end{aligned}$$

Thus,

$$h(\beta) = \beta^{114} + \beta^{57} + 1 = 0$$

and

$$h(x) \mid x^{114} + x^{57} + 1$$

where $h(x)$ is any one of the 6 self-reciprocal irreducible polynomials of degree 18. Thus, $T_{114,57}(x)$ has 6 degree 18 factors when multiplied together over $GF(2)$ yields a degree 108 polynomial.

The remaining degree 6 self-reciprocal polynomial is one of the following:

Self-Reciprocal Polynomials								Binary Coefficients of Factors
x^6	x^5	x^4	x^3	x^2	x	1		
(1)	1	0	0	1	0	0	1	irreducible
(2)	1	0	1	1	1	0	1	(1 1 1) (1 1 1 1 1)
(3)	1	1	0	1	0	1	1	(1 1 1) (1 1 1) (1 1 1)
(4)	1	1	1	1	1	1	1	(1 0 1 1) (1 1 0 1)

Polynomials (2) and (4) can be ruled out due to Corollaries 5.2 and 5.1, respectively. Since $T_{114,57}(x)$ is square-free, polynomial (3) cannot be a factor. Thus,

$$x^6 + x^3 + 1$$

with period 9 (and index 7) is the remaining factor. The irreducible factors of $T_{114,57}(x)$ are listed as follows:

Irreducible Factors of $T_{114,57}(x)$ in Octal	Degree of Factor	Period	Index
111	6	9	7
1055321	18	171	1533
1167671	18	171	1533
1315315	18	171	1533
1331155	18	171	1533
1505213	18	171	1533
1635347	18	171	1533

Note that β^{114} and β^{57} is the only CP among the 171 roots of unity. This is independent of the generation of the 171 roots of unity. Thus, applying the algorithm to each of the 6 self-reciprocal polynomials of degree 12 yields $T_{114,54}(x)$ as the trinomial of least degree containing the given self-reciprocal polynomial as a factor.

The polynomial $h_1(x)$ represented by 1055321 is listed in Appendix C of Reference 6 appended to its index 1533. The minimal polynomial $h_1(\beta^5) = 0$ was determined by a computer program to be $h_2(x)$ represented by 1167671, etc. The 6 self-reciprocal polynomials of degree 18 given in the foregoing table are listed in Reference 7. However, they are erroneously classified as primitive.

Golomb, in Reference 17, discusses irreducible polynomials, synchronization codes, and primitive necklaces in the context of cyclotomic algebra.

SECTION V

VERY LARGE SCALE INTEGRATED CIRCUIT CONSIDERATIONS

Switching elements comprise less than 10% of the active chip area of a Very Large Scale Integrated (VLSI) circuit chip. Interconnections make up the balance.

A static shift register is made up of identical stages or cells. Identical cells lead to a maximally regular topology in a VLSI layout known as a floor plan. The geometric design of one cell is replicated to a desired number to form a cascade. Each cell is a clocked memory element called a static flip-flop. The flip-flop is a bistable device capable of assuming one of two state-values.

A functional logic diagram of a JK flip-flop is shown in Figure 5-1. The state of the flip-flop is defined by its assertion output q at a particular CPI. The negation output is \bar{q} (the complement of q).

The logic inputs are J and K. A change in the state of the flip-flop can only occur after the application of a clock pulse denoted by C_p . The logical behavior of the JK flip-flop is reflected in the following state table:

J	K	q	Q
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

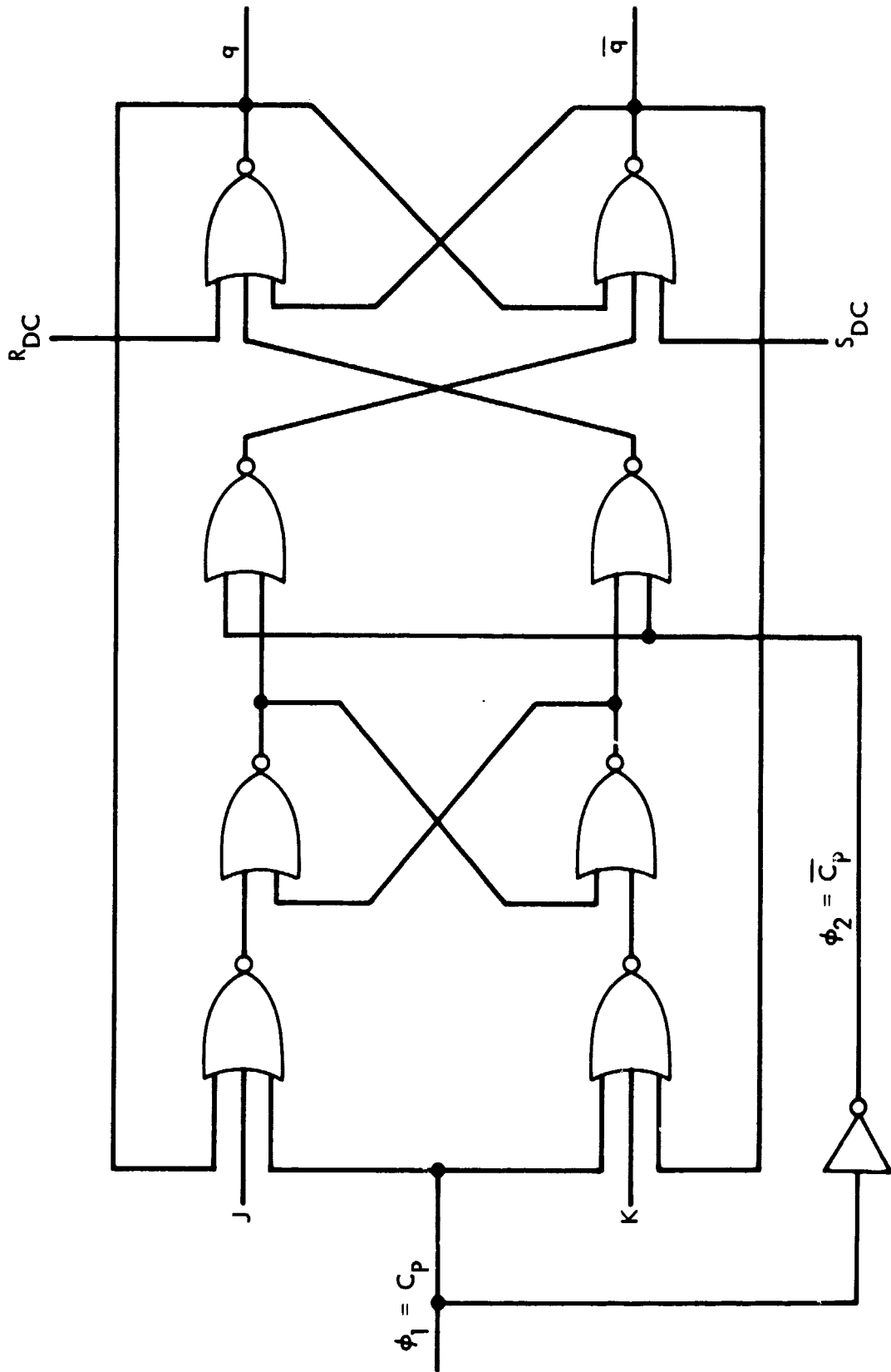


Figure 5-1. Master-Slave O-Enable JK Flip-Flop

J and K represent present inputs, and q represents the present (assertion) output or state of the flip-flop. Let k denote a CPI, the time between two consecutive clock pulses. Then,

$$q(k) \rightarrow q(k+1) = Q$$

where Q denotes the state the flip-flop assumes after the application of a clock pulse. Q is referred to as the next (assertion) output or state of the flip-flop. The next state Q is a Boolean function of J, K, and q. Expressed in minimal (logical) sum of (logical) products form

$$Q = \bar{J}\bar{q} \vee Kq \quad (31)$$

Juxtaposition denotes the logical product or the AND operation (e.g., K AND q is expressed as Kq). The symbol \vee denotes the OR (i.e., Inclusive-OR operation). A detailed presentation on switching (Boolean) functions and clocked memory elements appears in Reference 18. The reader is cautioned to note that the symbols for the OR and Exclusive-OR operations in Reference 18 differ from those in this report. Expression (31) is the characteristic function of the JK flip-flop. It is a Boolean difference equation where time dependency is implied.

Let $J = \bar{K}$ in (26). Then,

$$\begin{aligned} \bar{J} &= K \\ \text{and } Q &= K\bar{q} \vee Kq = K \end{aligned}$$

Thus, when inputs J and K are complementary, the next state Q, after the application of a clock pulse C_p , is the state-value of K prior to application of C_p . The assertion output, in effect, "copies" the state-value of K. The behavior of the JK flip-flop under the condition J equals \bar{K} is that of a D flip-flop (i.e., a delay flip-flop). Let q_i and \bar{q}_i denote the assertion and negation output of the i^{th} JK flip-flop in a cascade. Let J_{i+1} and K_{i+1} denote the respective inputs to the $(i + 1)$ th JK flip-flop whose

assertion output is q_{i+1} . Connecting q_i to K_{i+1} and \bar{q}_i to J_{i+1} results in shifting the content of the i^{th} flip-flop (i.e., q_i) to the $(i + 1)$ th flip-flop upon the application of a C_p .

The JK flip-flop in Figure 5-1 is comprised of 8 NOR (OR-NOT) gates and one inverter for developing a two-phase clock. The JK flip-flop is made up of two clocked cross-coupled NOR gates called latches. One serves as a master and is clocked by $\phi_1 = C_p$. The slave is clocked by $\phi_2 = \bar{C}_p$ (the complement of C_p). The state of the master is determined by the J and K inputs when $C_p = 0$, while the inputs to the slave are disabled $\bar{C}_p = 1$. The master (clocked latch) assumes a stable state prior to the time C_p becomes 1 as \bar{C}_p becomes 0. The state of the slave then assumes the state of the master during which time the inputs to the master (J and K) are disabled. Feedback from the assertion output q to the NOR gate, which has J and C_p as other inputs and feedback from the negation output \bar{q} to the NOR gate, which has K and C_p as other inputs provide input gate steering. Gate steering allows a state-value of 0 to simultaneously be applied to the J and K input. The J input when at state-value 0 (and $K = 1$) is a set input which causes the assertion output q to assume a state-value of 1 (via the slave). Whereas, the K input when at state-value 0 (and $J = 1$) is a clear (or reset) input which causes the assertion output, q , to assume a state-value of 0 (via the slave). When J and K are both at state-value 0, the state of the JK flip-flop changes. From (26)

$$\begin{aligned} Q &= \bar{J}\bar{q} \vee Kq \\ &= \bar{0}\bar{q} \vee 0q = \bar{q} \end{aligned}$$

Thus, $J = K = 0$ is a toggle input which is not employed in a shift register configuration. A $J = K = 1$ cause no change in q . A condensed state table of a 0-enable JK flip-flop is listed as follows:

J	K	Q
0	0	\bar{q}
0	1	1
1	0	0
1	1	q

The second and third entries where J and K are complementary correspond to D flip-flop behavior where Q copies the K input. S_{DC} and R_{DC} in Figure 5-1 are asynchronous set and clear inputs, respectively. S_{DC} when at state-value 1 sets the flip-flop, and R_{DC} when at state-value 1 resets the flip-flop.

$$S_{DC} R_{DC} = 0$$

is a constraint. That is, a state-value of 1 should not be applied to S_{DC} and R_{DC} simultaneously since q will assume an indeterminate state-value (i.e., \emptyset , a 0 or a 1). Both S_{DC} and R_{DC} override the clocked logical inputs J and K. The S_{DC} and R_{DC} inputs with added control logic provide a means for on-chip initialization of each flip-flop.

Another configuration of the 0 enable JK flip-flop where $J = K = T$ is of interest. From (26)

$$\begin{aligned} Q &= \bar{T}q \vee Tq = \bar{T} + q \\ &= 1 + T + q \end{aligned} \quad (32)$$

The next state Q is the complement of the Exclusive-OR of the T input and the present state q of the flip-flop. Connecting J and K inputs together results in a trigger or T flip-flop whose characteristic function is linear. In a subsequent report, it will be shown that the feedback of an SSFSR characterized by a trinomial may be reduced to a wire when the register

portion is made up of a combination of D and T flip-flops. The conditions under which the properties and the length of a given periodic sequence is preserved will be discussed.

An N channel Metal-Oxide-Semiconductor (NMOS) circuit of the 0-enable JK flip-flop appears in Figure 5-2. Each transistor is an N channel Metal-Oxide-Semiconductor Field-Effect Transistor (MOSFET). Those operating in the depletion mode serve as pull-ups and are labeled MD. Those operating in the enhancement mode are served as pull-downs and are labeled ME. The optimal length-to-width ratios of the gate geometries are discussed in Reference 19. The NOR gate configuration was chosen because its delay time for falling transitions is decreased as more or its inputs are active. Added stray capacitance does, however, offset this decrease.

A functional logic diagram of an on-stage SSFSR characterized by

$$T_{n,a}(X) = X^n + X^a + 1$$

is given in Figure 5-3. Clock and initialization circuitry is omitted. The two-level logic function comprised of three NOR gates is effectively a 2-input Exclusive-OR circuit. Thirty transistors comprise the NMOS cell (i.e., JK flip-flop) in Figure 5-2. Intracell connections are highly localized. Whereas, intercell connections are simply two wires due to the fact that the shift register is a serial device. The cellularity of a shift register and the serialization of intercell connections leads to topological regularity amenable to VLSI chip designs.

Introducing feedback to the shift register enhances its usefulness beyond all expectations of the early 1950s when independent discoveries were surfacing (Reference 3). The combinational logic in feedback of a shift register, however, adversely affects the topological layout of a VLSI design. This is particularly true in a SSFSR where a two-level linear-logic function grows sharply with the number of arguments (Reference 18). A feedback network with a single 2-input modulo 2 summer (i.e., Exclusive-OR gate) is the least

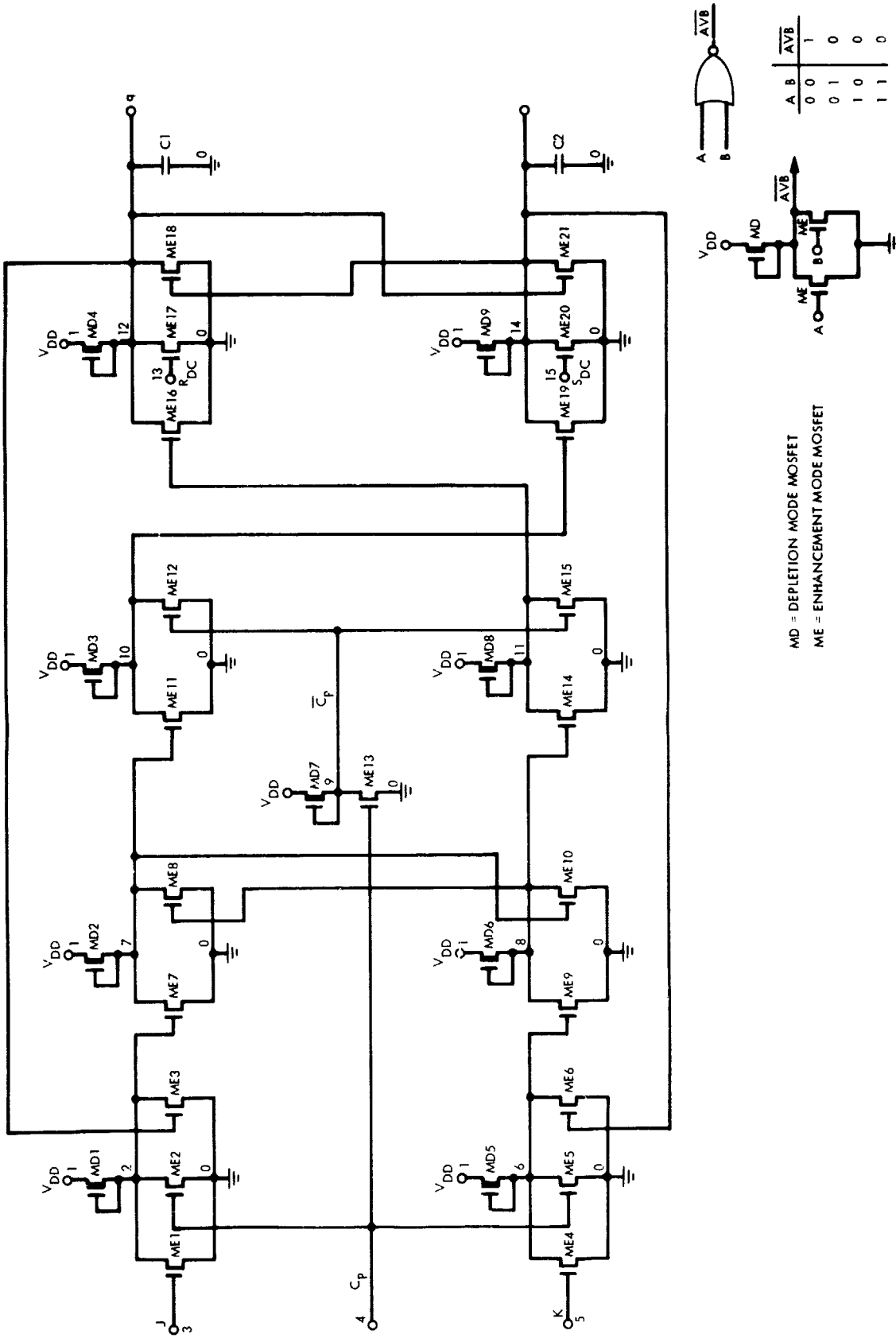
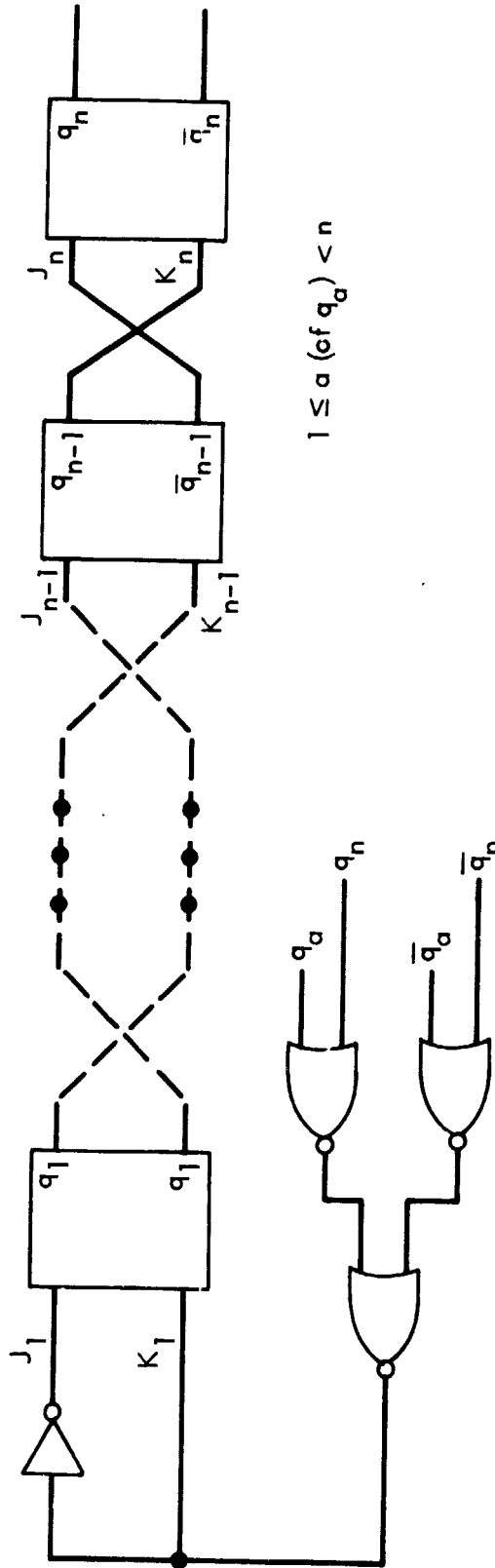


Figure 5-2. NMOS Circuit of a Static 0-Enable JK Flip-Flop

$$J_1 = \bar{q}_a + q_n = \bar{K}_1$$

$$K_1 = q_a + q_n$$

$$Q_1 = q_a + q_n$$



THE SYMBOL "+" DENOTES THE EXCLUSIVE - OR OPERATION

Figure 5-3. A Functional Logic Diagram of a n-Stage SSFSR Characterized by $X^n + X^a + 1$

complex without resulting in cycles (of states) of trivial length. Isomorphic SSFSR and ISFSR with such a feedback function are of identical complexity in terms of transistor count and propagation delay.

This report discusses the embedding of the behavior of an r-stage shift register with linear-logic feedback into that of an n-stage shift register with a single 2-input modulo summer in its feedback in Section IV. The sole purpose is to realize VLSI architecture of maximal regularity (i.e., identical cells) with intercell communications serialized to a maximal degree.

SECTION VI

SUMMARY

Feedback shift registers have proven to be efficient periodic binary sequence generators. Polynomials of degree r over a Galois Field characteristic 2 ($GF(2)$) characterize the behavior of shift registers with linear-logic feedback. Such FSRs are amenable to analysis and synthesis. Furthermore, the synthesis of shift registers with nonlinear feedback is often the result of "adding" nonlinear terms to a linear recurrence relation. See Reference 23 and Chapter VI entitled "Nonlinear Shift Register Sequences" in Reference 3.

Application of periodic binary sequences include random number generation (Reference 15), spread spectrum communications (Reference 20), and radar ranging (a forerunner of spread spectrum communications (Reference 11)), and VLSI testing (References 21 and 22).

Other applications of FSRs include encryption and decryption (Reference 23), algebraic error-detection and error-correction encoding and decoding (References 4 and 6), and FSR synthesis of sequential machines (Reference 24).

The vast intrinsic combinatorics of an FSR accounts for its varied and significant applications. This report deals solely with shift registers with linear-logic feedback (the SSFSR and ISFSR) characterized by polynomials over $GF(2)$. The objective is the algorithmic determination of the trinomial of lowest degree, when it exists, that contains a given irreducible polynomial over $GF(2)$ as a factor. It was proven that every primitive polynomial of degree r is a factor of $2^{r-1} - 1$ trinomials and the one of lowest degree is square-free. A sufficient, but not a necessary condition, was proven for a nonprimitive irreducible polynomial to be a factor of a trinomial. Methods for determining the initial state of a SSFSR and ISFSR required to generate the periodic sequence associated with a factor of the trinomial was given.

A measure of complexity of a binary periodic sequence is the length of the shift register with linear-logic feedback which, when properly initialized, can generate the sequence (see References 4 and 25). It is proposed that a measure of complexity of an irreducible polynomial is the degree of the trinomial of least degree, if it exists, that contains the irreducible polynomial as a factor.

SECTION VII

REFERENCES

1. Birkoff, G., and MacLane, S., A Survey of Modern Algebra, Revised Edition, The Macmillan Co., New York, 1953.
2. Golomb, S.W., "Theory of Transformation Groups of Polynomials over $GF(2)$ with Applications to Linear Shift Register Sequences," Information Sciences, Vol. 1, pp. 87-109, 1968.
3. Golomb, S.W., Shift Register Sequences, Revised Edition, Aegean Park Press, Laguna Hills, California, 1982.
4. Berlekamp, E.R., Algebraic Coding Theory, Revised 1984 Edition, Aegean Park Press, Laguna Hills, California, 1984.
5. Dean, R.A., Elements of Abstract Algebra, John Wiley and Sons, Inc., New York, 1966.
6. Peterson, W.W., and Weldon, Jr., E.J., Error-Correcting Codes, 2nd Edition, The M.I.T. Press, Cambridge, Massachusetts, 1972.
7. Marsh, R.W., Table of Irreducible Polynomials over $GF(2)$ through Degree 19, distributed by the Office of Technical Services, Commerce Department, Washington, D.C., October 1957.
8. Stahnke, W., "Primitive Binary Polynomials," Mathematics of Computation, Vol. 27, No. 124, pp. 997-980, October 1973.
9. Watson, E.J., "Primitive Polynomials (Mod 2)," Mathematics of Computation, Volume 16, pp. 368-369, 1962.

10. Lempel, A., "Analysis and Synthesis of Polynomials and Sequences over $GF(2)$," IEEE Transactions on Information Theory, Vol. IT-17, pp. 297-303, 1971.
11. Golomb, S.W., Editor, Digital Communications with Space Applications, Prentice Hall, Englewood Cliffs, New Jersey, 1964, Second Edition, Peninsula Publishing, Los Altos, California, 1982.
12. Zierler, N. and Brillhart, J., "On Primitive Trinomials (Mod 2)," Information and Control, Vol. 13, No.6, pp. 541-554, December, 1968.
13. Zierler, N., and Brillhart, J., "On Primitive Trinomials, (Mod 2) II," Information and Control, Vol. 14, No. 6, pp. 556-569, June 1969.
14. Swan, R.G., "Factorization of Polynomials over Finite Fields," Pacific Journal of Mathematics, Vol. 12, pp. 1099-1106, 1962.
15. Tausworthe, R.C., "Random Numbers Generated by Linear Recurrence Modulo Two," Mathematics of Computation, Vol. 19, pp. 201-209, 1965.
16. Feller, W., An Introduction to Probability Theory and Its Applications, Vol. 1, Third Edition, John Wiley and Sons, Inc., New York, 1968.
17. Golomb, S.W., "Irreducible Polynomials, Synchronization Codes, Primitive Necklaces, and the Cyclotomic Algebra," Combinatorial Mathematics and Its Applications, Chapter 21, Proc. of the 1st U.N.C. Conference Conf. on Combinatorial Mathematics and Its Applications., April, 1967, University of North Carolina Press, pp. 358-370, 1969.
18. Perlman, M., "Abstract Algebra," Encyclopedia of Computer Science and Technology, Marcel Dekker, Inc., New York, Vol. 1, pp. 1-102, 1975.
19. Mead, C., and Conway, L., Introduction to VLSI Systems, Addison-Wesley Publishing Co., Reading, Massachusetts, 1980.

20. Holmes, J.K., Coherent Spread Spectrum Communications Systems, John Wiley and Sons, Inc., New York, 1982.
21. Williams, T.W. and Parker, K.P., "Design for Testability - A Survey," Special Issue on VLSI Design: Problems and Tools, Proceedings of the IEEE, Vol. 7, No. 1, pp. 98-112, January 1983.
22. Tang, D.T., and Chen, C.-L., "Logic Test Pattern Generation Using Linear Codes," IEEE Transactions on Computers, Vol. C-33, No. 9, pp. 845-850, September 1984.
23. Perlman, M., "Generation of Key in Cryptographic System for Secure Communications," NASA Technical Brief No. B75-10278, October 1975.
24. Martin, R.L., Studies in Feedback Shift-Register Synthesis of Sequential Machines, Research Monograph No. 50, The M.I.T. Press Cambridge, Massachusetts, 1969.
25. Massey, J.L., "Shift Register Synthesis and BCH Decoding," IEEE Transactions on Information Theory, IT15, pp. 122-127, 1969.

APPENDIX A

NUMBER THEORETIC FUNCTIONS

APPENDIX A

NUMBER-THEORETIC FUNCTIONS

A number-theoretic function is any function that is defined over positive integral arguments. A number-theoretic function $f(m)$ is multiplicative if

$$f(ab) = f(a)f(b) \quad \text{whenever } (a,b) = 1$$

The prime-power factorization of a positive integer $m > 1$ is

$$m = \prod_{i=1}^k p_i^{e_i}$$

where k and e_i are positive integers and p_i prime integers. A prime is defined as an integer $p > 1$ that is divisible by 1 and p only. Thus, a multiplicative number-theoretic function over m may be expressed as

$$f(m) = f\left(\prod_{i=1}^k p_i^{e_i}\right) = \prod_{i=1}^k f\left(p_i^{e_i}\right)$$

since

$$\left(p_i^{e_i}, p_j^{e_j}\right) = 1 \quad \text{for } i \neq j$$

The Euler-phi function $\varphi(m)$ is defined as the number of positive integers no greater than m that are relatively prime to m . Furthermore, $\varphi(m)$

is multiplicative. The integers no greater than p^k that are not relatively prime to p^k are those that contain p as a factor, namely,

$$p, 2p, \dots, p^{k-1}p$$

There are a total of p^{k-1} such integers. Therefore,

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

The integer 1 is neither a prime nor a composite. To be complete, $\varphi(1)$ is defined to be 1.

In general,

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

As discussed in Section I, the number of primitive polynomials of degree r over $GF(2)$ is

$$\varphi(2^r - 1)/r$$

Also, the number of irreducible nonprimitive polynomials of degree r and period d over $GF(2)$ is $\varphi(d)/r$. The value of d is such that $d < 2^k - 1$ and d divides $2^k - 1$ for $k = r$, but does not divide $2^k - 1$ for $k < r$.

The set of all cosets (proper and improper) relative to the multiplicative subgroup

$$\{1, 2, 4, \dots, 2^{r-1}\}$$

correspond to the $2^r - 1$ roots of unity arranged into cyclotomic cosets.

The number of cyclotomic cosets is

$$N_c = \frac{1}{r} \left[\sum_{d|r} \varphi(d) 2^{r/d} \right] - 1$$

where $d|r$ denotes "d divides r." The summation is taken over all $d \geq 1$ that divide r.

Another multiplicative number-theoretic function of interest is the Möbius function denoted by $\mu(m)$. The Möbius function is defined by

$$\mu(m) = \begin{cases} 1 & \text{if } m = 1 \\ 0 & \text{if } a^2 | m \text{ for } a > 1 \\ (-1)^k & \text{if } m = p_1 p_2 \dots p_k \text{ where } p_i \text{ are distinct primes} \end{cases}$$

The Möbius function shows up frequently in number theory, particularly in the Möbius inversion formula. If f is any number-theoretic function, not necessarily multiplicative, and

$$F(m) = \sum_{d|m} f(d)$$

then

$$f(m) = \sum_{d|m} F(d)\mu(n/d) = \sum_{d|m} F(n/d)\mu(d)$$

The number of irreducible polynomials of degree r over GF(2) is I_r where

$$2^r = \sum_{d|r} d I_d$$

For $r = 6$, I_6 is determined recursively. Divisors of 6 are 1, 2, 3, and 6.

$$\begin{array}{ll}
2^1 = 1 \cdot I_1 & I_1 = 2 \\
2^2 = 2 + 2I_2 & I_2 = 1 \\
2^3 = 2 + 3I_3 & I_3 = 2 \\
2^6 = 2 + 2 + 6 + 6I_6 & I_6 = 9
\end{array}$$

A closed form for I_r follows from applying the Möbius inversion formulas.
For

$$F(r) = 2^r \quad \text{and} \quad f(d) = dI_d$$

$$rI_r = \sum_{d|r} 2^{r/d} \mu(d) \quad \text{and} \quad I_r = \frac{1}{r} \sum_{d|r} 2^{r/d} \mu(d)$$

For $r = 6$,

$$\mu(1) = 1, \mu(2) = -1, \mu(3) = -1, \mu(6) = 1$$

$$I_6 = \frac{1}{6} [2^6 - 2^3 - 2^2 + 2] = 9$$

The number-theoretic functions for determining the number of primitive and irreducible polynomials over $GF(2)$ is applicable to $GF(p)$. The number of primitive polynomials of degree r is a subset of I_r over $GF(p)$. That is,

$$\frac{\varphi(p^r - 1)}{r} \leq \frac{1}{r} \sum_{d|r} p^{r/d} \mu(d)$$

Equality arises only for the case of $GF(2)$ when $2^r - 1$ is prime. The reader is invited to see References 3, 4, and 17 for detailed presentations on $\varphi(m)$, $\mu(d)$, and the Möbius inversion formula.

APPENDIX B

**TRINOMIAL OF LEAST DEGREE THAT CONTAINS
A GIVEN PRIMITIVE POLYNOMIAL OF DEGREE
 r OVER $GF(2)$ AS A FACTOR**

APPENDIX B

TRINOMIAL OF LEAST DEGREE THAT CONTAINS A GIVEN PRIMITIVE
POLYNOMIAL OF DEGREE r OVER $GF(2)$ AS A FACTOR

r	COEFF. OF $f(x)$ IN OCTAL	$T(x)$		IRREDUCIBLE FACTORS OF $T(x)$ IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
		n	a				
<u>5</u>	<u>45</u>	<u>5</u>	<u>2</u>	<u>45</u>	<u>5</u>	<u>31</u>	<u>1</u>
	<u>67</u>	7	2	7 <u>67</u>	2 <u>5</u>	3 <u>31</u>	1 <u>1</u>
	<u>57</u>	8	3	13 <u>57</u>	3 <u>5</u>	7 <u>31</u>	1 <u>1</u>
<u>6</u>	<u>103</u>	<u>6</u>	<u>1</u>	<u>103</u>	<u>6</u>	<u>63</u>	<u>1</u>
	<u>133</u>	8	7	7 <u>133</u>	2 <u>6</u>	3 <u>63</u>	1 <u>1</u>
	<u>147</u>	11	8	73 <u>147</u>	5 <u>6</u>	31 <u>63</u>	1 <u>1</u>
<u>7</u>	<u>203</u>	<u>7</u>	<u>1</u>	<u>203</u>	<u>7</u>	<u>127</u>	<u>1</u>
	<u>211</u>	<u>7</u>	<u>3</u>	<u>211</u>	<u>7</u>	<u>127</u>	<u>1</u>
	<u>235</u>	10	9	15 <u>235</u>	3 <u>7</u>	7 <u>127</u>	1 <u>1</u>
	<u>277</u>	13	3	133 <u>277</u>	6 <u>7</u>	63 <u>127</u>	1 <u>1</u>
	<u>247</u>	14	13	7 45 <u>247</u>	2 5 <u>7</u>	3 31 <u>127</u>	1 1 <u>1</u>
	<u>253</u>	19	7	<u>253</u> 12067*	<u>7</u> 12	<u>127</u> 4095	<u>1</u> 1
	<u>217</u>	19	13	<u>217</u> 10663*	<u>7</u> 12	<u>127</u> 4095	<u>1</u> 1
	<u>357</u>	19	17	7 <u>357</u> 2035*	2 <u>7</u> 10	3 <u>127</u> 341	1 <u>1</u> 3

r	COEFF. OF f(x) IN OCTAL	T(x) n a		IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
7	<u>313</u>	21	18	<u>313</u>	7	<u>127</u>	<u>1</u>
				72127*	14	381	43
8	<u>537</u>	13	11	7	2	3	1
				15	3	7	1
				<u>537</u>	8	<u>255</u>	<u>1</u>
	<u>453</u>	13	12	67	5	31	1
				<u>453</u>	8	<u>255</u>	<u>1</u>
	<u>455</u>	16	15	<u>455</u>	8	<u>255</u>	<u>1</u>
				675*	8	85	3
	<u>543</u>	20	9	13	3	7	1
				<u>543</u>	8	<u>255</u>	<u>1</u>
				1055*	9	511	1
<u>435</u>	21	10	<u>435</u>	8	<u>255</u>	<u>1</u>	
			21615*	13	8191	1	
<u>515</u>	23	1	7	2	3	1	
			<u>515</u>	8	<u>255</u>	<u>1</u>	
			34641*	13	8191	1	
<u>717</u>	27	2	13	3	7	1	
			<u>717</u>	8	<u>255</u>	<u>1</u>	
			375715*	16	65535	1	
<u>607</u>	27	8	<u>607</u>	8	<u>255</u>	<u>1</u>	
			3745133*	19	524287	1	
9	<u>1021</u>	9	4	<u>1021</u>	9	<u>511</u>	<u>1</u>
	<u>1533</u>	11	7	7	2	3	1
				<u>1533</u>	9	<u>511</u>	<u>1</u>
<u>1333</u>	11	10	7	2	3	1	
				<u>1333</u>	9	<u>511</u>	<u>1</u>

r	COEFF. OF		T(x)		IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
	f(x) IN OCTAL	n	a					
2	<u>1157</u>	13	6	23	4	15	1	
				<u>1157</u>	2	<u>511</u>	<u>1</u>	
	<u>1473</u>	15	13	147	6	63	1	
				<u>1473</u>	2	<u>511</u>	<u>1</u>	
	<u>1207</u>	19	8	7	2	3	1	
				15	3	7	1	
				51	5	31	1	
				<u>1207</u>	2	<u>511</u>	<u>1</u>	
	<u>1175</u>	19	9	<u>1175</u>	2	<u>511</u>	<u>1</u>	
				2355*	10	341	3	
	<u>1055</u>	20	9	13	3	7	1	
				543*	8	255	1	
				<u>1055</u>	2	<u>511</u>	<u>1</u>	
	<u>1275</u>	26	1	7	2	3	1	
				15	3	7	1	
				<u>1275</u>	2	<u>511</u>	<u>1</u>	
				12515*	12	4095	1	
	<u>1267</u>	27	15	<u>1267</u>	2	<u>511</u>	<u>1</u>	
				1234653*	18	1533	171	
	<u>1517</u>	29	4	7	2	3	1	
				313	7	127	1	
				<u>1517</u>	2	<u>511</u>	<u>1</u>	
				7723*	11	2047	1	
	<u>1437</u>	29	7	7	2	3	1	
				75	5	31	1	
				<u>1437</u>	2	<u>511</u>	<u>1</u>	
				32461*	13	8191	1	
	<u>1137</u>	29	14	<u>1137</u>	2	<u>511</u>	<u>1</u>	
				4533443*	20	349525	1	
	<u>1033</u>	29	24	13	3	7	1	
				73	5	31	1	
				<u>1033</u>	2	<u>511</u>	<u>1</u>	
				17233*	12	1365	3	

r	COEFF. OF f(x) IN OCTAL	T(x) n	a	IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
2	<u>1243</u>	36	1	<u>1243</u>	2	<u>511</u>	<u>1</u>
				2257*	10	341	3
				540663*	17	131071	1
	<u>1131</u>	36	19	15	3	7	1
				<u>1131</u>	2	<u>511</u>	<u>1</u>
				171611245*	24	16777215	1
	<u>1225</u>	39	16	<u>1225</u>	2	<u>511</u>	<u>1</u>
				7137*	11	2047	1
				3411757*	19	524287	1
	<u>1617</u>	39	18	<u>1617</u>	2	<u>511</u>	<u>1</u>
				10011	12	45	91
				1540753*	18	1533	171
<u>1167</u>	41	33	325	7	127	1	
			<u>1167</u>	2	<u>511</u>	<u>1</u>	
			373334507*	25	33554431	1	
<u>1423</u>	44	41	13	3	7	1	
			31	4	15	1	
			<u>1423</u>	2	<u>511</u>	<u>1</u>	
			3323	10	1023	1	
			1635423*	18	262143	1	
<u>1257</u>	45	20	<u>1257</u>	2	<u>511</u>	<u>1</u>	
			1205764323423*	36	2555	26896077	
<u>1577</u>	55	50	7	2	3	1	
			23	4	15	1	
			31	4	15	1	
			<u>1577</u>	2	<u>511</u>	<u>1</u>	
			1627006717343*	36	2555	26896077	
<u>1317</u>	57	49	<u>1317</u>	2	<u>511</u>	<u>1</u>	
			13555371*	21			
			1004427273*	27			
<u>1063</u>	61	39	13	3	7	1	
			<u>1063</u>	2	<u>511</u>	<u>1</u>	
			11643	12	4095	1	
			2541445310153*	37			

r	COEFF. OF		T(x)		IRREDUCIBLE		DEGREE OF FACTOR	PERIOD	INDEX
	f(x) IN OCTAL	n	a	FACTORS OF T(x) IN OCTAL					
<u>10</u>	<u>2011</u>	<u>10</u>	3	<u>2011</u>	<u>10</u>	<u>1023</u>		<u>1</u>	
	<u>2627</u>	13	9	13 <u>2627</u>	3 <u>10</u>	7 <u>1023</u>		1 <u>1</u>	
	<u>2327</u>	14	3	23 <u>2327</u>	4 <u>10</u>	15 <u>1023</u>		1 <u>1</u>	
	<u>2475</u>	17	8	13 23 <u>2475</u>	3 4 <u>10</u>	7 15 <u>1023</u>		1 1 <u>1</u>	
	<u>2617</u>	17	13	7 75 <u>2617</u>	2 5 <u>10</u>	3 31 <u>1023</u>		1 1 <u>1</u>	
	<u>2157</u>	23	7	7 <u>2157</u> 6435*	2 <u>10</u> 11	3 <u>1023</u> 2047		1 <u>1</u> 1	
	<u>3133</u>	23	8	141 247 <u>3133</u>	6 7 <u>10</u>	63 127 <u>1023</u>		1 1 <u>1</u>	
	<u>2767</u>	24	11	<u>2767</u> 55753*	<u>10</u> 14	<u>1023</u> 16683		<u>1</u> 1	
	<u>2773</u>	26	3	75 <u>2773</u> 7173*	5 <u>10</u> 11	31 <u>1023</u> 2047		1 <u>1</u> 1	
	<u>2707</u>	32	31	7 <u>2707</u> 3067* 3607*	2 <u>10</u> 10 10	3 <u>1023</u> 1023 341		1 <u>1</u> 1 3	
	<u>3067</u>	32	31	7 2707* <u>3067</u> 3607*	2 10 <u>10</u> 10	3 <u>1023</u> <u>1023</u> 341		1 1 <u>1</u> 3	

r	COEFF. OF f(x) IN OCTAL	T(x) n	a	IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
<u>10</u>	<u>2347</u>	35	22	7	2	3	1
				141	6	63	1
				<u>2347</u>	<u>10</u>	<u>1023</u>	<u>1</u>
				430005*	17	131071	1
<u>2443</u>	37	18	<u>2443</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			1272414137*	27			
<u>2033</u>	39	37	23	4	15	1	
			1321	9	511	1	
			<u>2033</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			210435*	16	65535	1	
<u>2213</u>	40	11	7	2	3	1	
			13	3	7	1	
			<u>2213</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			347702607*	25	33544431	1	
<u>2415</u>	49	24	455	8	255	1	
			<u>2415</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			27371170361*	31	2147483647	1	
<u>2047</u>	49	36	211	7	127	1	
			<u>2047</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			43207520343*	32			
<u>2503</u>	49	45	57	5	31	1	
			1151	9	511	1	
			<u>2503</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			4445*	11	2047	1	
			46215*	14	16383	1	
<u>3177</u>	51	41	13	3	7	1	
			<u>3177</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			317313	16	21845	3	
			23644577	22			
<u>2305</u>	53	28	7	2	3	1	
			<u>2305</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			73707*	14	16383	1	
			1321420701*	27			

r	COEFF. OF f(x) IN OCTAL	T(x) n	a	IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
<u>10</u>	<u>3427</u>	55	14	7	2	3	1
				<u>3427</u>	<u>10</u>	<u>1023</u>	<u>1</u>
				241461026171065*	43		
	<u>2055</u>	55	28	<u>2055</u>	<u>10</u>	<u>1023</u>	<u>1</u>
				15317555*	21	2097152	1
				164050421*	24		
<u>2527</u>	57	30	1033	9	511	1	
			<u>2527</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			3465*	10	341	3	
			3507	10	1023	1	
			1022707*	18	1533	171	
<u>2553</u>	57	51	111	6	9	7	
			235	7	127	1	
			<u>2553</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			3301	10	1023	1	
			3367	10	341	3	
			43445*	14	381	43	
<u>3023</u>	60	41	15	3	7	1	
			<u>3023</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			5444507177561433*	47			
<u>2363</u>	61	9	1207	9	511	1	
			<u>2623</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			53623*	14	16383	1	
			2310747647*	28			
<u>2377</u>	65	6	13	3	7	1	
			<u>2377</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			6227*	11	2047	1	
			60575*	14	16383	1	
			1062067767*	27			
<u>2145</u>	65	34	7	2	3	1	
			13	3	7	1	
			<u>2145</u>	<u>10</u>	<u>1023</u>	<u>1</u>	
			2605	10	1023	1	
			3573	10	341	3	
			111041*	15	1057	31	
			135407*	15	1057	31	

r	f(x) OF	T(x)	
	INDEX 1	n	a
10	3337	79	73
	3117	83	14

r	COEFF. OF	T(x)		IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
	f(x) IN OCTAL	n	a				
11	<u>4005</u>	11	2	<u>4005</u>	11	<u>2047</u>	1
	<u>6673</u>	13	5	7 <u>6673</u>	2 11	3 <u>2047</u>	1 1
	<u>4565</u>	16	9	45 <u>4565</u>	5 11	31 <u>2047</u>	1 1
	<u>5235</u>	20	7	7 357 <u>5235</u>	2 7 11	7 127 <u>2047</u>	1 1 1
	<u>5675</u>	22	13	31 325 <u>5675</u>	4 7 11	15 127 <u>2047</u>	1 1 1
	<u>5613</u>	23	16	7 3661* <u>5613</u>	2 10 11	3 1023 <u>2047</u>	1 1 1
	<u>5337</u>	24	5	<u>5337</u> 24703*	11 13	<u>2047</u> 8191	1 1
	<u>4237</u>	25	24	163 561 <u>4237</u>	6 8 11	63 255 <u>2047</u>	1 1 1
	<u>4261</u>	26	5	<u>4261</u> 105621*	11 15	<u>2047</u> 32767	1 1
	<u>6747</u>	26	23	57 3375* <u>6747</u>	5 10 11	31 1023 <u>2047</u>	1 1 1

r	COEFF. OF		T(x)		IRREDUCIBLE		DEGREE OF FACTOR	PERIOD	INDEX
	f(x) IN OCTAL	n	a	FACTORS OF T(x) IN OCTAL					
<u>11</u>	<u>6277</u>	29	25	7	2		3	1	
				323	7		127	1	
				1713*	9		511	1	
				<u>6277</u>	<u>11</u>		<u>2047</u>	<u>1</u>	
<u>4671</u>	30	7	<u>4671</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			2313171*	19		524287	1		
<u>6367</u>	31	20	7	2		3	1		
			<u>6367</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			1147625*	18		262143	1		
<u>5025</u>	32	17	<u>5025</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			12575505*	21		2097151	1		
<u>5733</u>	33	14	23	4		15	1		
			<u>5733</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			1255515*	18		37449	7		
<u>5253</u>	33	27	<u>5253</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			24246667*	22		6141	683		
<u>4653</u>	37	12	<u>4653</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			460401267*	26					
<u>5373</u>	37	33	163	6		63	1		
			217	7		127	1		
			<u>5373</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			35147*	13		8191	1		
<u>5575</u>	38	3	235	7		127	1		
			455	8		255	1		
			<u>5575</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			13245*	12		4095	1		
<u>7137</u>	39	16	1225*	9		511	1		
			<u>7137</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			3411757*	19		524287	1		

r	COEFF. OF		T(x)		IRREDUCIBLE		DEGREE	PERIOD	INDEX
	f(x) IN	OCTAL	n	s	FACTORS OF T(x)	IN OCTAL			
11	<u>5477</u>	39	19	13	3		7	1	
				51	5		31	1	
				247	7		127	1	
				<u>5477</u>	<u>11</u>		<u>2047</u>	<u>1</u>	
				20213*	13		8191	1	
<u>5657</u>	39	24	111	6		9	7		
			<u>5657</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			24546213*	22		6141	683		
<u>5007</u>	39	28	67	5		31	1		
			<u>5007</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			64425725*	23		8388607	1		
<u>4767</u>	41	5	551	8		255	1		
			<u>4767</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			24577263*	22		4194303	1		
<u>6013</u>	43	6	23	4		15	1		
			155	6		63	1		
			<u>6013</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			24064321*	22		60787	69		
<u>4225</u>	43	11	7	2		7	1		
			75	5		31	1		
			<u>4225</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			250330363*	25		33554431	1		
<u>6447</u>	43	15	1207	9		511	1		
			3417	10		341	3		
			<u>6447</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			24637*	13		8191	1		
<u>4423</u>	47	11	13	3		7	1		
			<u>4423</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			126643071475*	33					
<u>5023</u>	47	39	13	3		7	1		
			31	4		15	1		
			1725	9		511	1		
			<u>5023</u>	<u>11</u>		<u>2047</u>	<u>1</u>		
			4772721*	20		1048575	1		

r	COEFF. OF		T(x)		IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
	f(x) IN OCTAL	n	a					
<u>11</u>	<u>6727</u>	48	21		67	5	31	1
					3453	10	93	11
					<u>6727</u>	<u>11</u>	<u>2047</u>	<u>1</u>
					34424513*	22	6141	683
<u>5357</u>	48	29		23	4	15	1	
				155	6	63	1	
				<u>5357</u>	<u>11</u>	<u>2047</u>	<u>1</u>	
				1456104075*	27			
<u>4365</u>	49	17		1	2	3	1	
				51	5	31	1	
				<u>4365</u>	<u>11</u>	<u>2047</u>	<u>1</u>	
				12165	12	4095	1	
				3321023*	19	524287	1	
<u>6307</u>	4	30		67	5	31	1	
				613	8	85	3	
				765	8	255	1	
				<u>6307</u>	<u>11</u>	<u>2047</u>	<u>1</u>	
				542667*	17	131017	1	
<u>4505</u>	49	39		<u>4505</u>	<u>11</u>	<u>2047</u>	<u>1</u>	
				117767*	15	4681	7	
				42000367*	23	8338607	1	
<u>4445</u>	49	45		57	5	31	1	
				1151	9	511	1	
				2503*	10	1023	1	
				<u>4445</u>	<u>11</u>	<u>2047</u>	<u>1</u>	
				46215*	14	16383	1	
<u>6557</u>	53	17		23	4	15	1	
				<u>6557</u>	<u>11</u>	<u>2047</u>	<u>1</u>	
				12727*	12	4095	1	
				615627213*	26			
<u>4107</u>	54	25		13	3	7	1	
				2047	10	1023	1	
				<u>4107</u>	<u>11</u>	<u>2047</u>	<u>1</u>	
				51303*	14	16383	1	
				232031*	16	13107	5	

r	COEFF. OF		T(x)		IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
	f(x) IN OCTAL	n	a					
<u>11</u>	<u>5557</u>	55	10		<u>5557</u> 577532413432723*	<u>11</u> 44	<u>2047</u>	<u>1</u>
	<u>4475</u>	56	41		57 1725 <u>4475</u> 37157355273*	5 7 <u>11</u> 31	31 511 <u>2047</u> 2147483647	1 1 <u>1</u> 1
	<u>4347</u>	51	11		23 <u>4347</u> 112443714550031*	4 <u>11</u> 42	15 <u>2047</u>	1 <u>1</u>
	<u>7237</u>	58	55		13 <u>7237</u> 731154217564031*	3 <u>11</u> 44	7 <u>2047</u>	1 <u>1</u>
	<u>4317</u>	59	25		7 <u>4317</u> 11103* 312004430753*	2 <u>11</u> 12 34	3 <u>2047</u> 1365	1 <u>1</u> 3
	<u>4353</u>	59	29		13 <u>4353</u> 26761* 40561341405*	3 <u>11</u> 13 32	7 <u>2047</u> 8191	1 <u>1</u> 1
	<u>4603</u>	61	43		15 73 1563 <u>4603</u> 75273* 2041035*	3 5 9 <u>11</u> 14 19	7 31 511 <u>2047</u> 16383 524287	1 1 1 <u>1</u> 1 1
	<u>6127</u>	64	47		7 15 <u>6127</u> 17141473700110531*	2 3 <u>11</u> 48	3 7 <u>2047</u>	1 1 <u>1</u>
	<u>6227</u>	65	6		13 2377* <u>6227</u> 60575* 1062067767*	3 10 <u>11</u> 14 27	7 1023 <u>2047</u> 16383	1 1 <u>1</u> 1

r	COEFF. OF		T(x)		IRREDUCIBLE		DEGREE	PERIOD	INDEX
	f(x) IN	OCTAL	n	a	FACTORS OF T(x)	IN OCTAL			
11	<u>4161</u>	65	7		7		2	3	1
					771		8	85	3
					<u>4161</u>		<u>11</u>	<u>2047</u>	<u>1</u>
					514561*		17	131071	1
					1101174323*		27		
<u>4563</u>	65	28		7		2	3	1	
				4553		<u>11</u>	<u>2047</u>	<u>1</u>	
				307036250332170431*		52			
<u>4145</u>	65	40		7		2	3	1	
				23		4	15	1	
				31		4	15	1	
				<u>4145</u>		<u>11</u>	<u>2047</u>	<u>1</u>	
				404454203214625*		44			
<u>4053</u>	68	3		<u>4053</u>		<u>11</u>	<u>2047</u>	<u>1</u>	
				452075*		17	131071	1	
				22540240100253*		40			
<u>5537</u>	68	55		7		2	3	1	
				<u>5537</u>		<u>11</u>	<u>2047</u>	<u>1</u>	
				3751431316172617015*		55			
<u>4473</u>	69	21		111		6	9	7	
				<u>4473</u>		<u>11</u>	<u>2047</u>	<u>1</u>	
				20342647*		22			
	10001101111*		30						
<u>4215</u>	69	41		271		7	127	1	
				<u>4215</u>		<u>11</u>	<u>2047</u>	<u>1</u>	
				4361545*		20		1	
				26622761641*		31	2147483647		

r	f(x) of		n	a	r	f(x) of		n	a
	INDEX	1				INDEX	1		
11	4055	71	14		11	5607	93	14	
	4173	71	47			5177	93	61	
	4415	71	56			6417	94	83	
	7047	71	68			5263	96	61	

r	f(x) of INDEX 1	n	a	r	f(x) of INDEX 1	n	a
11	4251	72	15	11	4655	97	90
	6153	73	17		6037	99	62
	4451	73	34		4027	100	35
	6163	73	40		5403	101	79
	5155	75	72		4577	101	82
	4617	79	39		5247	103	18
	6507	79	61		6637	107	85
	5747	81	38		5623	109	1
	7317	82	17		4143	109	27
	5265	82	23		4707	111	106
	4533	86	9		5463	117	25
	5513	88	75		6263	133	39
	4745	89	87		6233	142	99
					5667	143	12

r	COEFF. OF f(x) IN OCTAL	T(x) n	a	IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
<u>12</u>	<u>12067</u>	19	7	253*	7	127	1
				<u>12067</u>	<u>12</u>	<u>4095</u>	<u>1</u>
	<u>10663</u>	19	13	217*	7	127	1
				<u>10663</u>	<u>12</u>	<u>4095</u>	<u>1</u>
	<u>12753</u>	25	21	45	5	31	1
				573	8	85	3
				<u>12753</u>	<u>12</u>	<u>4095</u>	<u>1</u>
	<u>12515</u>	26	1	7	2	3	1
				15	3	7	1
				1275*	9	511	1
				<u>12515</u>	<u>12</u>	<u>4095</u>	<u>1</u>
	<u>10353</u>	31	29	7	2	3	1
				13	3	7	1
				<u>10353</u>	<u>12</u>	<u>4095</u>	<u>1</u>
				60147*	14	16383	1
	<u>10175</u>	34	5	7	2	3	1
				51	5	31	1
				<u>10175</u>	<u>12</u>	<u>4095</u>	<u>1</u>
				163767*	15	32767	1

r	COEFF. OF		T(x)		IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
	f(x) IN OCTAL	n	a					
<u>12</u>	<u>12117</u>	37	3		15	3	7	1
					345	7	127	1
					<u>12117</u>	<u>12</u>	<u>4095</u>	<u>1</u>
					120403*	15	32767	1
<u>12165</u>	37	30		<u>12165</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
				250303445*	25	33554431	1	
<u>12255</u>	38	35		271	7	127	1	
				551	8	255	1	
				<u>5755*</u>	<u>11</u>	<u>2047</u>	<u>1</u>	
				12255	12	4095	1	
<u>11177</u>	42	17		<u>11177</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
				11066515603*	30			
<u>10737</u>	47	13		7	2	3	1	
				<u>10737</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
				151421301615*	33			
<u>11643</u>	49	18		31	4	15	1	
				1713	9	511	1	
				7113	11	2047	1	
				<u>11643</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
				31273*	13	8191	1	
<u>11313</u>	50	9		<u>11313</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
				4502237720127*	38			
<u>11163</u>	53	16		7	2	3	1	
				73	5	31	1	
				<u>11163</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
				277357101057*	34			
<u>12727</u>	53	17		23	4	15	1	
				6557*	11	2047	1	
				<u>12727</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
				615627213*	26			
<u>16317</u>	55	1		357	7	127	1	
				<u>16317</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
				1264522723457*	36			

r	COEFF. OF f(x) IN OCTAL	T(x) n	a	IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
<u>12</u>	<u>11015</u>	55	8	7	2	3	1
				235	7	127	1
				<u>11015</u>	<u>12</u>	<u>4095</u>	<u>1</u>
				53043	14	5461	3
				7054651*	20	95325	11
<u>10731</u>	58	49	<u>10731</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
			2161250565777231*	46			
<u>11147</u>	60	25	<u>11147</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
			13223	12	819	5	
			13611*	12	4095	1	
			14227*	12	4095	1	
			16273*	12	4095	1	
<u>14227</u>	60	25	11147*	12	4095	1	
			13223	12	819	5	
			13611*	12	4095	1	
			<u>14227</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
			16273*	12	4095	1	
<u>11075</u>	60	35	<u>11075</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
			14455	12	819	5	
			15467*	12	4095	1	
			16311*	12	4095	1	
			16443*	12	4095	1	
<u>15467</u>	60	35	11075*	12	4095	1	
			14455	12	819	5	
			<u>15467</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
			16311*	12	4095	1	
			16443*	12	4095	1	
<u>11067</u>	64	1	23	4	15	1	
			11045	12	1365	3	
			<u>11067</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
			11441*	12	4095	1	
			11463	12	819	5	
			11515*	12	4095	1	

r	COEFF. OF f(x) IN OCTAL	T(x)		IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
		n	a				
<u>12</u>	<u>11515</u>	64	1	23	4	15	1
				11045	12	1365	3
				11067*	12	4095	1
				11441*	12	4095	1
				11463	12	819	5
				<u>11515</u>	<u>12</u>	<u>4095</u>	<u>1</u>
<u>12007</u>	64	27	<u>12007</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
			252442144723171333*	52			
<u>10231</u>	64	63	31	4	15	1	
			<u>10231</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
			12211	12	1365	3	
			13131*	12	4095	1	
			14631	12	819	5	
			16611*	12	4095	1	
<u>10605</u>	67	61	13	3	7	1	
			<u>10605</u>	<u>12</u>	<u>4095</u>	<u>1</u>	
			55317733*	23	8388608	1	
			4017247741*	29			

r	f(x) of INDEX 1	T(x)		r	f(x) of INDEX 1	T(x)	
		n	a			n	a
12	16027	70	29	12	13275	103	56
	15437	71	26		14433	103	57
	13677	71	41		10527	104	43
	11435	71	52		10123	107	97
	17057	72	19		16047	109	76
	12247	73	38		11477	109	91
	12323	78	53		13503	115	2
	12435	79	40		15033	117	80
	10173	80	43		14357	119	44
	15677	83	19		10407	125	94
	14573	83	73		16237	129	48
	10443	85	9		10473	135	53
	10553	85	67		11271	136	1
	14613	86	7		12735	145	108
	13663	87	72		12135	152	37
	14717	87	72		15527	153	75

r	f(x) of INDEX 1	T(x)		r	f(x) of INDEX 1	T(x)	
		n	a			n	a
12	10517	91	19	12	13107	161	84
	10437	91	64		12147	161	107
	11471	93	34		10321	162	151
	10151	93	52		14127	163	143
	12417	99	93		14747	164	113
	15053	101	67		11417	171	42
	12623	102	13				

r	f(x) of INDEX 1	$x^r f(1/x)$	T(x)		<u>FACTOR OF T(x) LISTED ELSEWHERE</u>			
			n	a	r	COEFF. IN OCTAL	PERIOD	INDEX
<u>13</u>	<u>25627</u>	<u>35165</u>	<u>16</u>	<u>3</u>				
	<u>22637</u>	<u>37151</u>	<u>18</u>	<u>1</u>				
	<u>21135</u>	<u>27221</u>	<u>20</u>	<u>1</u>				
	<u>21615</u>	<u>26161</u>	<u>21</u>	<u>10</u>	<u>8</u>	<u>435</u>	<u>255</u>	<u>1</u>
	<u>20547</u>	<u>34641</u>	<u>23</u>	<u>1</u>	<u>8</u>	<u>515</u>	<u>255</u>	<u>1</u>
	<u>23737</u>	<u>37371</u>	<u>23</u>	<u>4</u>				
	<u>24703</u>	<u>30345</u>	<u>24</u>	<u>5</u>	<u>11</u>	<u>5377</u>	<u>2047</u>	<u>1</u>
	<u>30057</u>	<u>36403</u>	<u>25</u>	<u>6</u>	<u>9</u>	<u>113</u>	<u>73</u>	<u>7</u>
	<u>23005</u>	<u>24031</u>	<u>25</u>	<u>9</u>				
	<u>24061</u>	<u>21405</u>	<u>27</u>	<u>11</u>				
	<u>25775</u>	<u>27765</u>	<u>29</u>	<u>6</u>	<u>16</u>	<u>266745</u>	<u>65535</u>	<u>1</u>
	<u>21453</u>	<u>32461</u>	<u>29</u>	<u>7</u>	<u>9</u>	<u>1437</u>	<u>511</u>	<u>1</u>
	<u>22075</u>	<u>27411</u>	<u>31</u>	<u>4</u>	<u>14</u>	<u>52547</u>	<u>5461</u>	<u>3</u>
	<u>20715</u>	<u>26341</u>	<u>31</u>	<u>5</u>	<u>16</u>	<u>337377</u>	<u>4369</u>	<u>15</u>
	<u>24513</u>	<u>32245</u>	<u>31</u>	<u>21</u>	<u>10</u>	<u>3277</u>	<u>341</u>	<u>3</u>

r	f(x) of INDEX 1	$x^r f(1/x)$	T(x)		FACTOR OF T(x) LISTED ELSEWHERE			
			n	a	r	COEFF. IN OCTAL	PERIOD	INDEX
<u>13</u>	<u>25333</u>	<u>33325</u>	<u>35</u>	<u>4</u>	<u>14</u>	<u>60367</u>	<u>16383</u>	<u>1</u>
	<u>34627</u>	<u>35147</u>	<u>37</u>	<u>33</u>	<u>11</u>	<u>5373</u>	<u>2047</u>	<u>1</u>
	<u>20213</u>	<u>32101</u>	<u>39</u>	<u>19</u>	<u>11</u>	<u>5477</u>	<u>2047</u>	<u>1</u>
	<u>24637</u>	<u>37145</u>	<u>43</u>	<u>15</u>	<u>11</u>	<u>6447</u>	<u>2047</u>	<u>1</u>
	<u>31273</u>	<u>33523</u>	<u>49</u>	<u>18</u>	<u>12</u>	<u>11643</u>	<u>4095</u>	<u>1</u>
	<u>21557</u>	<u>36661</u>	<u>50</u>	<u>31</u>	<u>12</u>	<u>16276</u>	<u>273</u>	<u>15</u>
	<u>21755</u>	<u>26761</u>	<u>59</u>	<u>29</u>	<u>11</u>	<u>4531</u>	<u>2047</u>	<u>1</u>
	<u>30357</u>	<u>36703</u>	<u>63</u>	<u>38</u>	<u>12</u>	<u>13377</u>	<u>819</u>	<u>5</u>
<u>14</u>	<u>66673</u>	<u>63777</u>	<u>16</u>	<u>5</u>				
	<u>45627</u>	<u>72351</u>	<u>17</u>	<u>2</u>				
	<u>55753</u>	<u>65755</u>	<u>24</u>	<u>11</u>	<u>10</u>	<u>2767</u>	<u>1023</u>	<u>1</u>
	<u>40275</u>	<u>57201</u>	<u>26</u>	<u>11</u>	<u>9</u>	<u>1027</u>	<u>511</u>	<u>1</u>
	<u>60147</u>	<u>71403</u>	<u>31</u>	<u>29</u>	<u>12</u>	<u>10353</u>	<u>4095</u>	<u>1</u>
	<u>42335</u>	<u>52621</u>	<u>32</u>	<u>11</u>	<u>18</u>	<u>1206221</u>	<u>262143</u>	<u>1</u>
	<u>60367</u>	<u>73603</u>	<u>35</u>	<u>4</u>	<u>13</u>	<u>25333</u>	<u>8191</u>	<u>1</u>
	<u>51145</u>	<u>51445</u>	<u>35</u>	<u>11</u>	<u>21</u>	<u>12624165</u>	<u>2097151</u>	<u>1</u>
	<u>42645</u>	<u>51321</u>	<u>38</u>	<u>11</u>				
	<u>46215</u>	<u>54231</u>	<u>49</u>	<u>45</u>	<u>10</u>	<u>2503</u>	<u>1023</u>	<u>1</u>
	<u>70767</u>	<u>73707</u>	<u>53</u>	<u>28</u>	<u>10</u>	<u>2305</u>	<u>1023</u>	<u>1</u>
	<u>51303</u>	<u>60645</u>	<u>54</u>	<u>25</u>	<u>11</u>	<u>4107</u>	<u>2047</u>	<u>1</u>
	<u>53623</u>	<u>62365</u>	<u>61</u>	<u>9</u>	<u>10</u>	<u>2363</u>	<u>1023</u>	<u>1</u>
	<u>67257</u>	<u>75273</u>	<u>61</u>	<u>43</u>	<u>11</u>	<u>4603</u>	<u>2047</u>	<u>1</u>

r	f(x) of INDEX 1	$x^r f(1/x)$	T(x)		FACTOR OF T(x) LISTED ELSEWHERE			
			n	a	r	COEFF. IN OCTAL	PERIOD	INDEX
<u>14</u>	<u>57503</u>	<u>60575</u>	<u>65</u>	<u>6</u>	<u>10</u>	<u>2377</u>	<u>1023</u>	<u>1</u>
	<u>40473</u>	<u>67101</u>	<u>66</u>	<u>37</u>	<u>12</u>	<u>12315</u>	<u>585</u>	<u>7</u>
<u>15</u>	<u>100003</u>	<u>140001</u>	<u>15</u>	<u>1</u>				
	<u>100021</u>	<u>100201</u>	<u>15</u>	<u>4</u>				
	<u>100201</u>	<u>100401</u>	<u>15</u>	<u>7</u>				
	<u>134567</u>	<u>167235</u>	<u>18</u>	<u>5</u>				
	<u>104657</u>	<u>172621</u>	<u>19</u>	<u>3</u>				
	<u>103653</u>	<u>134741</u>	<u>23</u>	<u>3</u>				
	<u>121563</u>	<u>147305</u>	<u>25</u>	<u>12</u>				
	<u>104721</u>	<u>105621</u>	<u>26</u>	<u>5</u>	<u>11</u>	<u>4261</u>	<u>2047</u>	<u>1</u>
	<u>163327</u>	<u>165547</u>	<u>31</u>	<u>14</u>				
	<u>117143</u>	<u>143171</u>	<u>33</u>	<u>8</u>				
	<u>153677</u>	<u>176753</u>	<u>33</u>	<u>8</u>				
	<u>163767</u>	<u>167747</u>	<u>34</u>	<u>5</u>	<u>12</u>	<u>11735</u>	<u>4095</u>	<u>1</u>
	<u>113625</u>	<u>124751</u>	<u>34</u>	<u>13</u>	<u>19</u>	<u>2257305</u>	<u>524287</u>	<u>1</u>
	<u>102643</u>	<u>142641</u>	<u>35</u>	<u>6</u>	<u>20</u>	<u>7664741</u>	<u>1048575</u>	<u>1</u>
<u>15</u>	<u>120403</u>	<u>140205</u>	<u>37</u>	<u>3</u>	<u>12</u>	<u>12117</u>	<u>4095</u>	<u>1</u>
	<u>145453</u>	<u>152323</u>	<u>45</u>	<u>3</u>				
	<u>123453</u>	<u>152345</u>	<u>45</u>	<u>12</u>				
	<u>123433</u>	<u>154435</u>	<u>45</u>	<u>21</u>				
	<u>113637</u>	<u>174751</u>	<u>47</u>	<u>41</u>	<u>12</u>	<u>11737</u>	<u>1365</u>	<u>1</u>
<u>16</u>	<u>263677</u>	<u>375715</u>	<u>27</u>	<u>2</u>	<u>8</u>	<u>717</u>	<u>255</u>	<u>1</u>

r	f(x) of INDEX 1	x ^r f(1/x)	T(x)		FACTOR OF T(x) LISTED ELSEWHERE			
			n	a	r	COEFF. IN OCTAL	PERIOD	INDEX
<u>16</u>	<u>266745</u>	<u>247555</u>	<u>29</u>	<u>6</u>	<u>13</u>	<u>27765</u>	<u>8191</u>	<u>1</u>
	<u>306313</u>	<u>323143</u>	<u>36</u>	<u>13</u>	<u>16</u>	<u>372705</u>	<u>21845</u>	<u>3</u>
	<u>210435</u>	<u>270421</u>	<u>39</u>	<u>37</u>	<u>10</u>	<u>2033</u>	<u>1023</u>	<u>1</u>
	<u>274577</u>	<u>376475</u>	<u>40</u>	<u>13</u>				
<u>17</u>	<u>400011</u>	<u>440001</u>	<u>17</u>	<u>3</u>				
	<u>400041</u>	<u>410001</u>	<u>17</u>	<u>5</u>				
	<u>400101</u>	<u>404001</u>	<u>17</u>	<u>6</u>				
	<u>666673</u>	<u>673333</u>	<u>19</u>	<u>5</u>				
	<u>431277</u>	<u>772461</u>	<u>22</u>	<u>5</u>				
	<u>454765</u>	<u>537151</u>	<u>22</u>	<u>7</u>				
	<u>443573</u>	<u>675611</u>	<u>25</u>	<u>11</u>				
	<u>437265</u>	<u>532761</u>	<u>29</u>	<u>10</u>				
	<u>431455</u>	<u>551461</u>	<u>29</u>	<u>3</u>				
	<u>436407</u>	<u>701361</u>	<u>34</u>		<u>11</u>			
	<u>441715</u>	<u>547411</u>	<u>35</u>	<u>8</u>	<u>18</u>	<u>1352111</u>	<u>262143</u>	<u>1</u>
	<u>430005</u>	<u>500061</u>	<u>35</u>	<u>22</u>	<u>10</u>	<u>2033</u>	<u>1023</u>	<u>1</u>
	<u>540663</u>	<u>633015</u>	<u>36</u>	<u>1</u>	<u>10</u>	<u>2257</u>	<u>1023</u>	<u>1</u>
	<u>542667</u>	<u>733215</u>	<u>49</u>	<u>30</u>	<u>11</u>	<u>6307</u>	<u>2047</u>	<u>1</u>
	<u>437771</u>	<u>477761</u>	<u>50</u>	<u>17</u>	<u>12</u>	<u>13773</u>	<u>1365</u>	<u>3</u>
	<u>452075</u>	<u>570271</u>	<u>68</u>	<u>3</u>	<u>11</u>	<u>4053</u>	<u>2047</u>	<u>1</u>
<u>18</u>	<u>1000201</u>	<u>1004001</u>	<u>18</u>	<u>7</u>				
	<u>1147625</u>	<u>1247631</u>	<u>31</u>	<u>20</u>	<u>11</u>	<u>6367</u>	<u>2047</u>	<u>1</u>

r	f(x) of INDEX 1	$x^r f(1/x)$	T(x)		FACTOR OF T(x) LISTED ELSEWHERE			
			n	a	r	COEFF. IN OCTAL	PERIOD	INDEX
<u>18</u>	<u>1044604</u>	<u>1206221</u>	<u>32</u>	<u>11</u>	<u>14</u>	<u>52621</u>	<u>16383</u>	<u>1</u>
	<u>1110535</u>	<u>1352111</u>	<u>35</u>	<u>8</u>	<u>17</u>	<u>547411</u>	<u>131071</u>	<u>1</u>
	<u>1037433</u>	<u>1543741</u>	<u>37</u>	<u>1</u>	<u>19</u>	<u>342043</u>	<u>524287</u>	<u>1</u>
	<u>1443347</u>	<u>1635423</u>	<u>44</u>	<u>41</u>	<u>9</u>	<u>1423</u>	<u>511</u>	<u>1</u>
<u>19</u>	<u>2713457</u>	<u>3647235</u>	<u>22</u>	<u>3</u>				
	<u>2327423</u>	<u>3107531</u>	<u>23</u>	<u>2</u>				
	<u>2352103</u>	<u>3021271</u>	<u>27</u>	<u>7</u>	<u>8</u>	<u>477</u>	<u>85</u>	<u>3</u>
	<u>3322477</u>	<u>3745133</u>	<u>27</u>	<u>8</u>	<u>8</u>	<u>607</u>	<u>255</u>	<u>1</u>
	<u>2746113</u>	<u>3221475</u>	<u>28</u>	<u>11</u>				
	<u>2516543</u>	<u>3065625</u>	<u>29</u>	<u>21</u>	<u>10</u>	<u>2437</u>	<u>341</u>	<u>3</u>
	<u>2313171</u>	<u>2363231</u>	<u>30</u>	<u>7</u>	<u>11</u>	<u>4671</u>	<u>2047</u>	<u>1</u>

APPENDIX C

TRINOMIAL OF LEAST DEGREE THAT CONTAINS
A GIVEN IRREDUCIBLE NONPRIMITIVE POLYNOMIAL
OF DEGREE r OVER $GF(2)$ AS A FACTOR

APPENDIX C

TRINOMIAL OF LEAST DEGREE THAT CONTAINS
A GIVEN IRREDUCIBLE NONPRIMITIVE POLYNOMIAL
OF DEGREE r OVER $GF(2)$ AS A FACTOR

r	COEFF. OF $h(x)$ IN OCTAL	$T(x)$ n a		IRREDUCIBLE FACTORS OF $T(x)$ IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
6	<u>111</u>	6	3	<u>111</u>	6	2	7
	<u>127</u>	9	6	13	3	7	1
				<u>127</u>	6	<u>21</u>	<u>3</u>
8	<u>567</u>	11	5	13	3	7	1
				<u>567</u>	8	<u>85</u>	<u>3</u>
	<u>573</u>	16	1	551*	8	255	1
				<u>573</u>	8	<u>85</u>	<u>3</u>
	<u>477</u>	27	7	<u>477</u>	8	<u>85</u>	<u>3</u>
				2352103*	19	524287	1
	<u>613</u>	33	18	13	3	7	1
				127	6	21	3
				561	8	255	1
				607	8	255	1
				<u>613</u>	8	<u>85</u>	<u>3</u>
	<u>433</u>	34	17	7	2	3	1
				<u>433*</u>	8	<u>51</u>	<u>5</u>
				661*	8	51	5
				637	8	51	5
			763*	8	51	5	
<u>637</u>	34	17	7	2	3	1	
			433*	8	51	5	
			661*	8	51	5	
			<u>637</u>	8	<u>51</u>	<u>5</u>	
			763*	8	51	5	
2	<u>1003</u>	2	1	<u>1003</u>	2	<u>73</u>	7
	<u>1145</u>	17	10	7	2	3	1
				147	6	63	1
			<u>1145</u>	2	<u>73</u>	7	

r	COEFF. OF		T(x)		IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
	h(x) IN OCTAL	n	a					
2	<u>1113</u>	25	6	15	3	7	1	
				<u>1113</u>	2	<u>73</u>	7	
				36403*	13	8191	1	
	<u>1027</u>	26	11	13	3	7	1	
				<u>1027</u>	2	<u>73</u>	7	
				57201*	14	16383	1	
10	<u>3247</u>	15	6	73	5	31	1	
				<u>3247</u>	10	<u>93</u>	11	
				2355	9	511	1	
	<u>2355</u>	10	<u>341</u>	3				
	<u>2035</u>	19	17	7	2	3	1	
				357*	7	127	1	
				<u>2035</u>	10	<u>341</u>	3	
	<u>2413</u>	21	15	57	5	31	1	
				111	6	9	7	
				<u>2413</u>	10	<u>93</u>	11	
	<u>2251</u>	22	11	7	2	3	1	
				<u>2251</u>	10	<u>33</u>	31	
				3043*	10	33	31	
	<u>3043</u>	22	11	7	2	3	1	
				2251*	10	33	31	
				<u>3043</u>	10	<u>33</u>	31	
	<u>2065</u>	24	15	13	3	7	1	
				45	5	31	1	
				127	6	21	3	
				<u>2065</u>	10	<u>93</u>	11	
	<u>2633</u>	26	9	2633	10	<u>341</u>	3	
				272107*	16	21845	3	
	<u>2437</u>	29	21	2437	10	<u>341</u>	3	
				2516543*	19	524287	1	

r	COEFF. OF		T(x)		IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
	h(x) IN OCTAL	n	a					
<u>10</u>	<u>3277</u>	31	21	537	8	255	1	
				<u>3277</u>	<u>10</u>	<u>341</u>	<u>3</u>	
				32245*	13	8191	1	
<u>3417</u>	32	1	7	2	3	1		
			<u>3417</u>	<u>10</u>	<u>341</u>	<u>3</u>		
			3435*	10	1023	1		
			3543*	10	1023	1		
			1243*	9	511	1		
<u>2257</u>	36	1	<u>2257</u>	<u>10</u>	<u>341</u>	<u>3</u>		
			540663*	17	131071	1		
			13	3	7	1		
<u>2017</u>	48	23	217	7	127	1		
			<u>2017</u>	<u>10</u>	<u>341</u>	<u>3</u>		
			2654016113*	28				
			75	5	31	1		
<u>2107</u>	55	22	<u>2107</u>	<u>10</u>	<u>341</u>	<u>3</u>		
			2671	10	341	3		
			3255*	10	341	3		
			3315	10	341	3		
			3367*	10	341	3		
			2107*	10	341	3		
			2671	10	341	3		
<u>3367</u>	55	22	75	5	31	1		
			2107*	10	341	3		
			2671	10	341	3		
			3255*	10	341	3		
			3315	10	341	3		
			3367	10	341	3		
			3367	10	341	3		
<u>2653</u>	55	33	57	5	31	1		
			2355	10	341	3		
			2633	10	341	3		
			<u>2653</u>	<u>10</u>	<u>341</u>	<u>3</u>		
			3421*	10	341	3		
			3573*	10	341	3		
			3573*	10	341	3		

r	COEFF. OF h(x) IN OCTAL	T(x) n	a	IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
10	<u>2547</u>	57	27	1541	9	511	1
				<u>2547</u>	10	<u>341</u>	3
				3427	10	1023	1
				3525*	10	1023	1
				1616441*	18	1533	171
2143	68	61	7	2	3	1	
			<u>2143</u>	10	<u>341</u>	3	
			6421727313*13061551*	56			

r	COEFF. OF h(x) IN OCTAL	PERIOD	INDEX	T(x) n	a
10	2123	341	3	75	62
	2231	341	3	78	19

r	COEFF. OF h(x) IN OCTAL	T(x) n	a	IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
12	<u>10011</u>	12	3	<u>10011</u>	12	<u>45</u>	<u>91</u>
	<u>10041</u>	12	5	<u>10041</u>	12	<u>819</u>	<u>5</u>
<u>13627</u>	15	10	13	3	7	1	
			<u>13627</u>	12	<u>35</u>	<u>117</u>	
<u>14537</u>	17	16	7	2	3	1	
			15	3	7	1	
			<u>14537</u>	12	<u>273</u>	<u>15</u>	
<u>11637</u>	23	11	51	5	31	1	
			133	6	63	1	
			<u>11637</u>	12	<u>585</u>	<u>7</u>	
<u>13617</u>	26	13	7	2	3	1	
			<u>13617</u>	12	<u>39</u>	<u>105</u>	
			17075*	12	39	105	

r	COEFF. OF $h(x)$ IN OCTAL	$T(x)$ n	s	IRREDUCIBLE FACTORS OF $T(x)$ IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
12	<u>10555</u>	28	21	23	4	15	1
				<u>10555</u>	<u>12</u>	<u>105</u>	<u>39</u>
				11073*	12	105	39
	<u>11073</u>	28	21	23	4	15	1
				10555*	12	105	39
				<u>11073</u>	<u>12</u>	<u>105</u>	<u>39</u>
	<u>15457</u>	29	5	15	3	7	1
				67	5	31	1
				1541*	9	511	1
				<u>15457</u>	<u>12</u>	<u>1365</u>	<u>3</u>
	<u>14373</u>	30	5	133	6	63	1
				<u>14373</u>	<u>12</u>	<u>315</u>	<u>13</u>
				15125*	12	315	13
	<u>12513</u>	30	25	155	6	63	1
				<u>12513</u>	<u>12</u>	<u>315</u>	<u>13</u>
				15743*	12	315	13
	<u>11727</u>	33	31	<u>11727</u>	<u>12</u>	<u>1365</u>	<u>3</u>
				13554513*	21	2097151	1
	<u>13003</u>	39	13	15	3	7	1
				11721*	12	91	45
				<u>13003</u>	<u>12</u>	<u>91</u>	<u>45</u>
				15173*	12	91	45
	<u>15173</u>	39	13	15	3	7	1
				11721*	12	91	45
				13003*	12	91	45
				<u>15173</u>	<u>12</u>	<u>91</u>	<u>45</u>
	<u>10571</u>	39	26	13	3	7	7
				<u>10571</u>	<u>12</u>	<u>91</u>	<u>45</u>
				14015*	12	91	45
				15713*	12	91	45

C-3

r	COEFF. OF h(x) IN OCTAL	T(x) n	a	IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
12	<u>11105</u>	40	5	7	2	3	1
				23	4	15	1
				31	4	15	1
				147	6	63	1
				<u>11105</u>	<u>12</u>	<u>315</u>	<u>13</u>
				16547*	12	315	13
<u>16327</u>	40	35	7	2	3	1	
			23	4	15	1	
			31	4	15	1	
			163	6	63	1	
			12111*	12	315	13	
			<u>16327</u>	<u>12</u>	<u>315</u>	<u>13</u>	
<u>12133</u>	41	10	7	2	3	1	
			<u>12133</u>	<u>12</u>	<u>1365</u>	<u>3</u>	
			1601624601*	27			
<u>11657</u>	43	16	<u>11657</u>	<u>12</u>	<u>1365</u>	<u>3</u>	
			23757171023*	31	2147483647	1	
<u>11045</u>	44	35	221	7	127	1	
			<u>11045</u>	<u>12</u>	<u>1365</u>	<u>3</u>	
			202314645*	25			
<u>13157</u>	46	43	<u>13157</u>	<u>12</u>	<u>585</u>	<u>7</u>	
			255372610323*	34			
<u>11735</u>	47	41	75	5	31	1	
			163	6	63	1	
			1707	9	511	1	
			<u>11735</u>	<u>12</u>	<u>1365</u>	<u>3</u>	
			174751*	15	32767	1	
<u>13773</u>	50	17	13	3	7	1	
			<u>13773</u>	<u>12</u>	<u>1365</u>	<u>3</u>	
			477761*	17	131071	1	
			1151665*	18	87381	3	

r	COEFF. OF h(x) IN OCTAL	T(x) n	a	IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
12	<u>16267</u>	50	31	7	2	3	1
				13	3	7	1
				<u>16267</u>	<u>12</u>	<u>273</u>	<u>15</u>
				36661*	13	8191	1
				6435053*	20		
<u>11463</u>	51	3	15	3	7	1	
			<u>11463</u>	<u>12</u>	<u>1365</u>	<u>3</u>	
			14455*	12	819	5	
			17235	12	1365	3	
			17403*	12	819	5	
<u>13223</u>	51	48	13	3	7	1	
			111	6	9	7	
			127	6	21	3	
			<u>13223</u>	<u>12</u>	<u>819</u>	<u>5</u>	
			14037*	12	819	5	
			14631*	12	819	5	
<u>14037</u>	51	48	13	3	7	1	
			111	6	9	7	
			127	6	21	3	
			13223*	12	819	5	
			<u>14037</u>	<u>12</u>	<u>819</u>	<u>5</u>	
			14631*	12	819	5	
<u>13143</u>	51	49	313	7	127	1	
			<u>13143</u>	<u>12</u>	<u>585</u>	<u>7</u>	
			73716032155*	32			
<u>10065</u>	52	13	31	4	15	1	
			<u>10065</u>	<u>12</u>	<u>195</u>	<u>21</u>	
			15347*	12	195	21	
			16701*	12	195	21	
			17277*	12	195	21	
<u>15347</u>	52	13	31	4	15	1	
			1065*	12	195	21	
			<u>15347</u>	<u>12</u>	<u>195</u>	<u>21</u>	
			16701*	12	195	21	
			17277*	12	195	21	

r	COEFF. OF		T(x)		IRREDUCIBLE		DEGREE OF FACTOR	PERIOD	INDEX
	h(x) IN OCTAL	n	a	FACTORS OF T(x) IN OCTAL					
12	<u>17277</u>	52	13	31	4	15	1		
				10065*	12	195	21		
				15347*	12	195	21		
				16701*	12	195	21		
				<u>17277</u>	<u>12</u>	<u>195</u>	<u>21</u>		
	<u>10167</u>	52	39	23	4	15	1		
				<u>10167</u>	<u>12</u>	<u>195</u>	<u>21</u>		
				12601*	12	195	21		
				16353*	12	195	21		
				17657*	12	195	21		
<u>10027</u>	55	15	45	5	31	1			
			141	6	63	1			
			<u>10027</u>	<u>12</u>	<u>315</u>	<u>13</u>			
			17513*	12	315	13			
			4454725	20	155	6765			
<u>15137</u>	55	40	51	5	31	1			
			103	6	63	1			
			<u>15137</u>	<u>12</u>	<u>315</u>	<u>13</u>			
			16401*	12	315	13			
			5271511	20	155	6765			
<u>16457</u>	56	33	357	7	127	1			
			<u>16457</u>	<u>12</u>	<u>1365</u>	<u>3</u>			
			254375*	16	4369	15			
			10416231*	21					
<u>16017</u>	57	14	<u>16017</u>	<u>12</u>	<u>1365</u>	<u>3</u>			
			1212717*	18	87381	3			
			1601251105*	27					
<u>12673</u>	59	17	<u>12673</u>	<u>12</u>	<u>585</u>	<u>7</u>			
			5162322607102347*	47					
<u>11103</u>	59	25	7	2	3	1			
			4317*	11	2047	1			
			<u>11103</u>	<u>12</u>	<u>1365</u>	<u>3</u>			
			312004430753*	34					

r	COEFF. OF h(x) IN OCTAL	T(x) n	a	IRREDUCIBLE FACTORS OF T(x) IN OCTAL	DEGREE OF FACTOR	PERIOD	INDEX
12	<u>13377</u>	63	38	<u>13377</u>	12	<u>819</u>	<u>5</u>
				36703*	13	8191	1
				7210220000101*	38		
<u>12315</u>	66	37		15	3	7	1
				765	8	255	1
				1715	9	511	1
				<u>12315</u>	<u>12</u>	<u>585</u>	<u>7</u>
				67101*	14	16383	1
				5267531*	20		
<u>10317</u>	67	20		7	2	3	1
				15	3	7	1
				<u>10317</u>	<u>12</u>	<u>273</u>	<u>15</u>
				42527114525216661*	50		

r	COEFF OF h(x) IN OCTAL	PERIOD	INDEX	T(x) n	a
12	10467	819	5	70	3
	13475	1365	3	76	69
	10377	117	35	78	39
	13413	117	35	78	39
	16757	117	35	78	39
	10063	819	5	78	65
	10115	819	5	78	65
	10243	819	5	78	65
	11031	819	5	78	65
	11673	819	5	82	33
	10461	273	15	82	53
	13077	273	15	83	46
	13113	585	7	83	69
	12265	1365	3	85	5
	13033	1365	3	85	5
	14667	1365	3	85	35
	12153	585	7	89	21
	12177	819	5	92	57
	13563	585	7	93	61
	10743	273	15	97	11
	13303	819	5	97	69
	11763	1365	3	99	29

r	COEFF OF h(x) IN OCTAL	PERIOD	INDEX	n	T(x)	a
12	11545	1365	3	102	53	
	13347	819	5	104	13	
	14513	819	5	104	13	
	11265	819	5	107	14	
	14177	585	7	107	96	
	13363	1365	3	109	81	
	11433	585	7	116	83	
	10245	585	7	118	87	
	14007	1365	3	122	35	
	13737	1365	3	125	103	
	13527	1365	3	126	115	
	10653	819	5	139	133	
	10077	1365	3	145	123	
	10355	1365	3	146	61	
	14043	585	7	156	39	
	10757	1365	3	160	109	
	10603	455	9	195	65	
	11703	455	9	195	65	
	11765	455	9	195	65	
	12023	455	9	195	65	
	15617	455	9	195	65	
	10213	455	9	195	130	
	11023	455	9	195	130	
	12337	455	9	195	130	
	13517	455	9	195	130	
	14313	455	9	195	130	
	14557	455	9	195	130	
	16137	455	9	195	130	
	14067	1365	3	217	201	