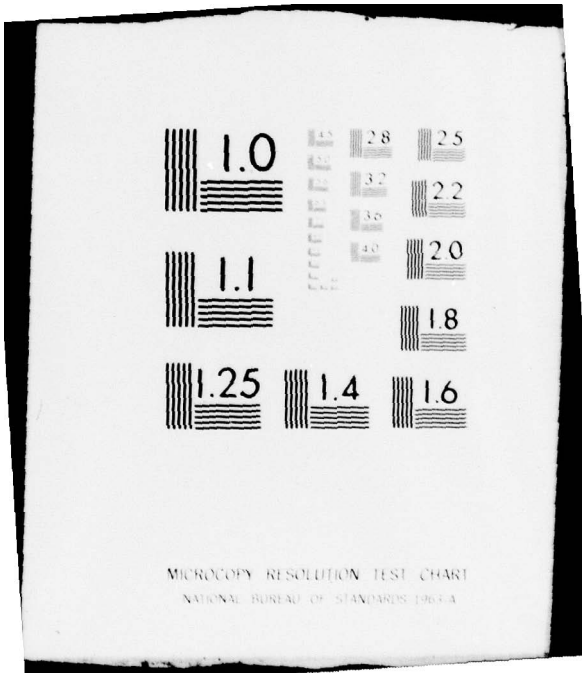
AD-A074 604 NAVAL WEAPONS CENTER CHINA LAKE CA F/G 9/4
SYNTHESIS OF SPREAD SPECTRUM SIGNALS FROM THE NON-BINARY GALOIS--ETC(U)
MAY 78 W O ALLTOP
UNCLASSIFIED NWC-TM-3475 GIDEP-E117-0706 NL

1 OF 1
AD A074604

END
DATE FILMED
11-79
DDC


1.0
1.1
1.25
1.4
1.6
2.0
2.2
2.5
2.8
3.2
3.6
4.0
1.8
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963-A

E117-0706

(9) NWC Technical Memorandum 3475

(1) LEVEL II

(14) NWC-TM-3475

AD A074604

(6) SYNTHESIS OF SPREAD SPECTRUM SIGNALS FROM THE NON-BINARY GALOIS FIELDS

by

(10) W. O. Alltop
Systems Development Department

(11) May 1978

(12) 40

(18) GIDEP

(19) E117-0706

Approved for public release; distribution unlimited.

NAVAL WEAPONS CENTER
China Lake, California 93555

403 019

JOB
C

1978

GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM

GENERAL DOCUMENT SUMMARY SHEET

1 OF 1

Please Type All Information – See Instructions on Reverse

1. ACCESS NUMBER: E117-0706	2. COMPONENT/PART NAME PER GIDEP SUBJECT THESAURUS: General Technical Data, Theoretical Analysis	
3. APPLICATION: Engineering	4. MFR NOTIFICATION: ☐ NOTIFIED ☒ NOT APPLICABLE	5. DOCUMENT ISSUE (Month/Year): May 1978
6. ORIGINATOR'S DOCUMENT TITLE: Synthesis of Spread Spectrum Signals from the Non-Binary Galois Fields		7. DOCUMENT TYPE: ☒ GEN RPT ☐ NONSTD PART ☐ SPEC
8. ORIGINATOR'S DOCUMENT NUMBER: NWC TM 3475	9. ORIGINATOR'S PART NAME/IDENTIFICATION: N/A	
10. DOCUMENT (SUPERSEDES) (SUPPLEMENTS) ACCESS NO.: None	11. ENVIRONMENTAL EXPOSURE CODES: N/A	
12. MANUFACTURER: N/A	13. MANUFACTURER PART NUMBER: N/A	14. INDUSTRY/GOVERNMENT STANDARD NUMBER: N/A

15. OUTLINE, TABLE OF CONTENTS, SUMMARY, OR EQUIVALENT DESCRIPTION

Maximal linearly recurring sequences over GF(p) are used to construct periodic, polyphase, spread spectrum signals, for p any odd prime. Sequences over GF(q), where q is a power of p, are also employed in the synthesis of pairs and triples of orthogonal signals. The orthogonal signals are ternary, utilizing the two phases 0 and π as well as intervals of shutdown. Spectral properties of the ternary codes are discussed. The difficulties of high-speed generation of linear sequences for odd primes are also presented. Although the linear sequences over GF(p) have been known for at least four decades, they have not yet been as well exploited in signal design as have binary sequences.

16. KEY WORDS FOR INDEXING: Recurring Sequences; Ternary Codes; Shift Registers; Spread Spectrum Signals (Doc Des--P)

17. GIDEP REPRESENTATIVE: M. H. Sloan	18. PARTICIPANT ACTIVITY AND CODE: Naval Weapons Center, China Lake, CA (X7)

DD FORM 1 OCT 77 2000

40

1

CONTENTS

3

1. INTRODUCTION

The well known binary PN (pseudo-noise) codes have been used for radar ranging, detection and communications systems for more than 20 years.[1] These codes are based on certain binary sequences. The two symbols 0,1 are associated with the phases 0 and π, giving rise to a biphase modulated signal.

$$F(t) = \sin(2\pi f_o t + \phi_k) \quad \text{for} \quad k \leq t < k + 1$$

The phase ϕ_k is 0 or π depending upon whether the k^{th} element x_k in the binary sequence is 0 or 1; f_o is the carrier frequency.

It is well known that each polynomial $f(\theta)$, which is primitive of degree m over the finite field GF(2), containing only 0 and 1, determines a binary sequence of period $L\ [=2^m - 1]$.[2,3] Each such sequence is an MLRS (maximal linearly recurring sequence) over GF(2). This terminology arises from the following facts. Each bit (element) of such a sequence is a linear sum of the preceding m bits. The coefficients in the polynomial $f(\theta)$ are the multipliers in the linear sum. Such sequences are maximal, because the period $2^m - 1$ is the largest achievable by an m^{th} degree polynomial.

As an example, let $f(\theta) = \theta^4 - a_1\theta^3 - a_2\theta^2 - a_3\theta - a_4$, with $(a_1, a_2, a_3, a_4) = (0, 0, 1, 1)$. The quartic $f(\theta) = \theta^4 - \theta - 1$ is primitive over GF(2). The associated MLRS is (0 0 0 1 0 0 1 1 0 1 0 1 1 1 1) with period 15:

---

[1] *Digital Communications With Space Applications*, ed. by S. W. Golomb. New York, Prentice Hall, 1964.

[2] S. W. Golomb. *Shift Register Sequences*. San Francisco, Holden-Day, 1967.

[3] W. W. Peterson and E. W. Weldon. *Error-correcting Codes*, 2nd ed. Cambridge, The M.I.T. Press, 1972.

$x_1 = 0$	$x_6 = 0$	$x_{11} = 0$
$x_2 = 0$	$x_7 = 1$	$x_{12} = 1$
$x_3 = 0$	$x_8 = 1$	$x_{13} = 1$
$x_4 = 1$	$x_9 = 0$	$x_{14} = 1$
$x_5 = 0$	$x_{10} = 1$	$x_{15} = 1$

For every k, $x_k = a_1x_{k-1} + a_2x_{k-2} + a_3x_{k-3} + a_4x_{k-4} = x_{k-3} + x_{k-4}$, using modulo 2 addition.

The desirability of the binary MLRS for correlation radar applications stems from three basic features:

1. The spectral lines of the code appear at almost all multiples of the word frequency f_w.
2. The normalized auto-correlation of the associated ±1 sequence has side lobes of magnitude 1/L.
3. The codes can be efficiently generated by shift registers using binary adders and flip-flops.

Thus, the PN codes are an important class of spread spectrum signals. The mathematical derivation and properties of the binary MLRS's have been known for at least four decades.[4,5] These properties hold, with slight modifications, for MLRS's over all finite fields $GF(q)$ of odd characteristic. For any power $q = p^r$ of an odd prime p, a primitive polynomial $f(\theta)$ of degree m over $GF(q)$ determines an MLRS of period $q^m - 1$ with symbols from $GF(q)$.

Our main objective here is to use these MLRS's over fields of odd characteristic p for the design of periodic spread spectrum signals. Two different types of signals are discussed: ternary biphase, and polyphase.

Using a linear (m=1) primitive polynomial, a (p-1)-phase signal of period p-1 results.[6] For large primes ($2^{31} - 1$ for example) these same sequences are used as uniform pseudo-random number generators in in digital computers.[7] In Section 2 ternary sequences are constructed

---

[4] J. Singer. "A Theorem in Finite Projective Geometry and Some Applications to Number Theory," *Amer. Math. Soc., Trans.*, Vol. 43 (1938), pp. 377-385.

[5] M. Hall. "An Isomorphism Between Linear Recurring Sequences and Algebraic Rings," *Amer. Math. Soc., Trans.*, Vol. 44 (1938), pp. 196-218.

[6] J. M. Alsup and J. M. Speiser. "Exponential Residue Codes," *IEEE Trans. Aerospace and Elec. Sys.*, November, 1975, pp. 1389-1390.

[7] D. E. Knuth. *The Art of Computer Programming*. Vol. 2, Seminumerical Algorithms. Reading, Mass., Addison-Wesley, 1969.

from every MLRS of odd characteristic p with degree $m \geq 2$. The resulting radar signal is biphase with the addition of shutdown intervals corresponding to zero bits in the MLRS. The shutdown intervals cause some loss of power, but the auto-correlation sidelobes are zero. In Section 3, p-phase signals are constructed from the MLRS's over GF(p). Whereas GF(q), $q = p^r > p$, can be used for ternary codes, the polyphase codes come only from GF(p), p an odd prime. The p-phase codes of Section 3 generalize the (p-1)-phase codes to degree m greater than one.[6]

Section 4 deals with spectral properties of the ternary codes and their products. Of the three distinct types of ternary codes defined in Section 3, two are negacyclic. (A negacyclic code of period $2M$ consists of an M-bit word followed by it negative.) The spectral lines for a negacyclic code occur at frequencies different from those of its products. The product spectra differ from those of binary PN codes, since the ternary codes do not possess the "shift and add" property. In Section 5, the shift registers over GF(q) are discussed. Two ternary codes for GF(9), $m = 2$, are given in Appendix A. These codes of period 20 and 40 are the shortest ones arising from fields $GF(p^r)$, $r > 1$.

A short discussion of irreducible trinomials over GF(3) is given in Appendix B.

2. TERNARY CODES

An odd characteristic sequence (OC sequence) is a sequence $\underline{s} = (s_i)$ of 0's, +1's, and -1's of period $Q = 2(q^m - 1)/(q - 1)$, with auto-correlation sequence $\underline{S} = (2q^{m-1}, 0, 0, \ldots, 0, -2q^{m-1}, 0, 0, \ldots, 0)$, where q is the power of an odd prime number p, and the coefficient $-2q^{m-1}$ occurs at position $Q/2$ in $\underline{S}$. For correlation purposes such sequences can be considered to have period $Q/2$ and perfect auto-correlation. The shortest nontrivial OC sequence is for $q = 3$ and $m = 2$. In this case $Q = 8$, $\underline{s} = (0 + + - 0 - - +)$, and $\underline{S} = (6, 0, 0, 0, -6, 0, 0, 0)$, as shown in Figure 1. The OC sequences, and others derived from them, are intimately related to near-difference sets and relative difference sets in cyclic groups.[8]

In cases where $Q/2$ is odd (equivalently m is odd), the sequence $\underline{s}^{(\frac{1}{2})} = (s_0, s_2, s_4, \ldots)$ of period $Q/2$ has auto-correlation $\underline{S}^{(\frac{1}{2})} = (q^{m-1}, 0, 0, \ldots)$. Furthermore, $-\underline{s}^{(\frac{1}{2})} = (s_1, s_3, s_5, \ldots)$ is the "other half" of $\underline{s}$. In addition to having perfect auto-correlations, the

---

[8] J. H. E. Elliott and A. T. Butson. "Relative Difference Sets," *Ill. J. Math.*, Vol. 10 (1966), pp. 517-531.

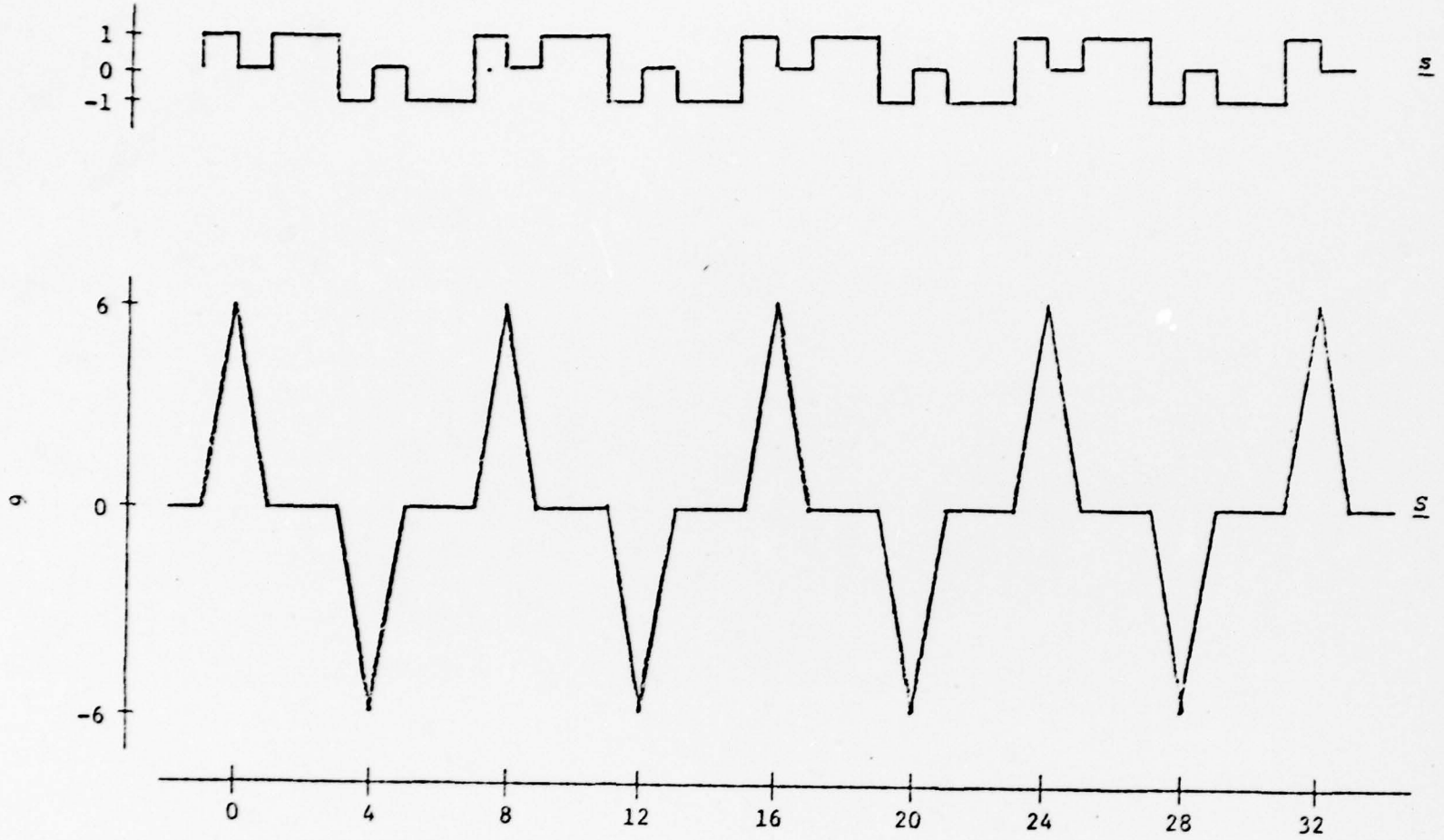


FIGURE 1. The Shortest OC Sequence $\underline{s}$, for $q = 3$, $m = 2$. Sequence period = 8, effective autocorrelation period = 4.

pair of sequences $\underline{s}$, $\underline{s}^{(\frac{1}{2})}$ are orthogonal, that is, have cross-correlation which is 0 everywhere, when integrated over Q bits.

For $q \equiv 1 \pmod 4$, an $OC^{(2)}$ sequence $\underline{s}^{(2)} = (s_i^{(2)})$ of period $2Q$ exists with auto-correlation $\underline{S}^{(2)} = (4q^{m-1}, 0, 0, \ldots, 0, -4q^{m-1}, 0, 0, \ldots, 0)$, the coefficient $-4q^{m-1}$ occurring at position Q in $\underline{S}^{(2)}$. Here $\underline{s}^{(2)}$ and $\underline{s}$ are also orthogonal over all $2Q$ bits. When $q \equiv 1 \pmod 4$ and m is odd, the triple $\underline{s}^{(2)}$, $\underline{s}$, $\underline{s}^{(\frac{1}{2})}$ are pairwise orthogonal when cross-correlated over $2Q$ bits.

The OC sequences are constructed from maximal linearly recurring sequences over the finite fields of odd characteristic. If

$$f(\vartheta) = \vartheta^m - a_1\vartheta^{m-1} - a_2\vartheta^{m-2} - \ldots - a_{m-1}\vartheta - a_m$$

is a polynomial over GF(q), then the associated linearly recurring sequence is defined by

$$(x_0, x_1, \ldots, x_{m-1}) = (0, 0, \ldots, 1),$$

$$x_k = a_1x_{k-1} + \ldots + a_mx_{k-m} \quad \text{for} \quad k \geq m.$$

Example 1. Let $f(\vartheta) = \vartheta^2 + \vartheta + 2$ over GF(5). The associated linearly recurring sequence $\underline{x}$ for $f(\vartheta)$ has period 24,

$$\underline{x} = (0\ 1\ 4\ 4\ 3\ 4\ 0\ 2\ 3\ 3\ 1\ 3\ 0\ 4\ 1\ 1\ 2\ 1\ 0\ 3\ 2\ 2\ 4\ 2).$$

Each bit of $\underline{x}$ satisfies $x_i \equiv 4x_{i-1} + 3x_{i-2} \pmod 5$.

The sequence $\underline{x}$ of Example 1 is, in fact, a maximal linearly recurring sequence of degree 2 over GF(5). It is a linearly recurring sequence by definition. It is maximal, that is, of maximal period, because there are only $24 = 5^2 - 1$ nonzero pairs from GF(5), the zero pair being (0,0). Each of these pairs occurs exactly once as a subsequence of consecutive bits in $\underline{x}$.

Recall that the period of an OC sequence is $Q = 2(q^m - 1)/(q - 1)$. In Example 1 the period of $\underline{x}$ is 24, while $2(5^2 - 1)/(5 - 1) = 12$. The OC sequence $\underline{s}$ derived from $\underline{x}$ is formed by a mapping $GF(5) \longrightarrow (-1, 0, +1)$. In particular

$$\begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 \\ + \\ - \\ - \\ + \end{bmatrix}$$

This gives

$$\underline{s} = (0 + + + - + 0 - - - + -),$$

$$\underline{S} = (10, 0, 0, 0, 0, 0, -10, 0, 0, 0, 0, 0),$$

where $\underline{S}$ is the auto-correlation sequence for $\underline{s}$.

More generally, an OC sequence $\underline{s}$ is derived from a maximal linearly recurring sequence $\underline{x}$ over GF(q) by the mapping

$$x_i \longrightarrow \begin{cases} -1 & \text{if } x_i \text{ is a quadratic nonresidue in GF(q)} \\ 0 & \text{if } x_i = 0 \\ +1 & \text{if } x_i \text{ is a nonzero quadratic residue in GF(q)} \end{cases}$$

A quadratic residue in a finite field is simply an element which possesses a square root. In the fields $GF(2^m)$ of even characteristic, every element has exactly one square root, since the mapping $a \longrightarrow a^2$ is a field automorphism. In the field GF(q) of odd characteristic, of the $q-1$ nonzero elements $(q-1)/2$ are squares and $(q-1)/2$ are not. Each nonzero square a^2 has the two square roots a and $-a$. (Recall that $a = -a$ in $GF(2^m)$.) In GF(5) the nonzero quadratic residues (squares) are 1 and $4 = -1$, while the nonresidues are 2 and $3 = -2$. Therefore, 1 and 4 are mapped into +1, while 2 and 3 are mapped into -1, as indicated above.

Example 2. Let $f(\theta) = \theta^2 + \theta + 3$ over GF(7), and let $\underline{x}$ and $\underline{s}$ be the associated maximal linearly recurring sequence and OC sequence of periods 48 and 16, respectively.

$$\underline{x} = (0\ 1\ 6\ 5\ 5\ 1\ 5\ 6\ 0\ 3\ 4\ 1\ 1\ 3\ 1\ 4\ 0\ 2\ 5\ 3\ 3\ 2\ 3\ 5\ 0$$

$$6\ 1\ 2\ 2\ 6\ 2\ 1\ 0\ 4\ 3\ 6\ 6\ 4\ 6\ 3\ 0\ 5\ 2\ 4\ 4\ 5\ 4\ 2),$$

$$\underline{s} = (0 + - - - + - - 0 - + + + - + +)$$

The nonzero quadratic residues in GF(7) are 1, 2, and 4, while the nonresidues are 3, 5, and 6.

The reduction in period from $\underline{x}$ to $\underline{s}$ deserves some discussion. Suppose the period of a linear recurring sequence over GF(q) is N. There exists a smallest divisor d of N such that $x_{i+d} = ax_i$ for all i and some fixed a in GF(q). Then $a^e = 1$, where de = N. In Example 2, d = 8, a = 3, and e = 6. For a maximal linearly recurring sequence of degree m over GF(q), the following conditions always hold.

$$d = (q^m-1)/(q-1),$$

a is a primitive root of GF(q),

$$e = q-1$$

Suppose q is odd, a primitive root a in GF(q) has no square root. For if $a = b^2$, then the element b has exponent 2(q-1), which is too large for a field with only q-1 nonzero elements. Since $x_{i+d} = ax_i$, it follows that x_{i+d} is a quadratic nonresidue if and only if x_i is a nonzero quadratic residue. This implies that $s_{i+d} = -s_i$, for all i, and $\underline{s}$ has period $2d = 2(q^m-1)/(q-1)$. Only in the case q = 3 do $\underline{x}$ and $\underline{s}$ have the same period $3^m - 1$.

Example 3. Let $f(\theta) = \theta^3 + 2\theta + 1$ over GF(3), and let $\underline{x}$ and $\underline{s}$ be the associated maximal linearly recurring sequence and OC sequence, respectively, both having period 26.

$$\underline{x} = (0\ 0\ 1\ 0\ 1\ 2\ 1\ 1\ 2\ 0\ 1\ 1\ 1\ 0\ 0\ 2\ 0\ 2\ 1\ 2\ 2\ 1\ 0\ 2\ 2\ 2),$$

$$\underline{s} = (0\ 0\ +\ 0\ +\ -\ +\ +\ -\ 0\ +\ +\ +\ 0\ 0\ -\ 0\ -\ +\ -\ -\ +\ 0\ -\ -\ -)$$

From Example 3 an $OC^{(\frac{1}{2})}$ sequence $\underline{s}^{(\frac{1}{2})}$ may be obtained, since $Q/2 = 26/2 = 13$ is odd,

$$\underline{s}^{(\frac{1}{2})} = (0\ +\ +\ +\ -\ +\ +\ 0\ 0\ +\ -\ 0\ -)$$

Figure 2 shows $s^{(\frac{1}{2})}$ and its auto-correlation function $\underline{S}^{(\frac{1}{2})}$.

The sequence $\underline{s}^{(\frac{1}{2})}$ may also be derived from the (nonmaximal) linearly recurring sequence $\underline{x}^{(\frac{1}{2})}$ associated with the polynomial $g(\theta) = \theta^3 + \theta^2 + \theta + 2$

$$\underline{x}^{(\frac{1}{2})} = (0\ 1\ 1\ 1\ 2\ 1\ 1\ 0\ 0\ 1\ 2\ 0\ 2)$$

As might be expected, $g(\theta)$ is a nonprimitive irreducible polynomial whose roots are the squares of the roots of $f(\theta)$ in GF(27). Cross-correlation of $\underline{s}$ and $\underline{s}^{(\frac{1}{2})}$ gives all 0's, since $s_{i+13} = -s_i$. The correlation of the first copy of a shift of $\underline{s}^{(\frac{1}{2})}$ against the first half of $\underline{s}$ is cancelled by the correlation of the second copy of $\underline{s}^{(\frac{1}{2})}$ against the second half of $\underline{s}$.

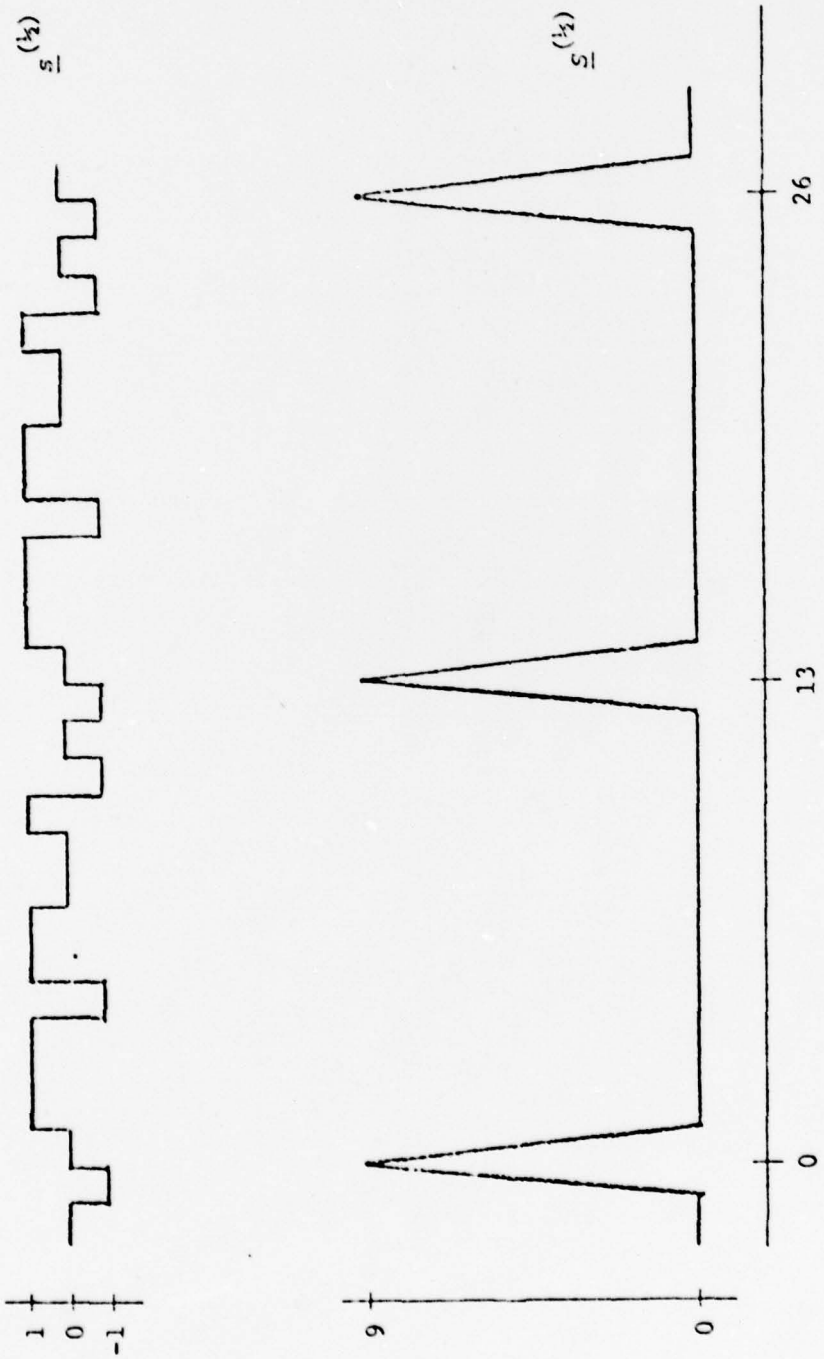


FIGURE 2. The Shortest $OC^{(\frac{1}{2})}$ Sequence $\underline{s}^{(\frac{1}{2})}$, for q = 3, m = 3. Sequence period = effective auto-correlation period = 13.

11

An $OC^{(2)}$ sequence is derived from a maximal linearly recurring sequence over GF(q) in much the same way as an OC sequence. A different mapping from GF(q) to (-1, 0, +1) is required. Let BI denote the set of nonzero biquadratic residues in GF(q). BI consists of those nonzero elements which are fourth powers in GF(q). For $q \equiv 1 \pmod 4$ and $a = b^4$ in GF(q), the four fourth roots of a are b, jb, -b, and -jb, where j and -j are the two square roots of -1. If c is a primitive root of GF(q), then the four sets BI, cBI, c^2BI, and c^3BI form a partition of the nonzero elements of GF(q) into four disjoint sets of size $(q-1)/4$. In this partition $BI \cup c^2BI$ is the set of nonzero quadratic residues of GF(q), while $cBI \cup c^3BI = c(BI \cup c^2BI)$ is the set of quadratic nonresidues. The $OC^{(2)}$ sequence $\underline{s}^{(2)}$ of period $2Q = 4(q^m-1)/(q-1)$ is the image of the maximal linearly recurring sequence $\underline{x}$ under the mapping

$$x_i \longrightarrow \begin{cases} +1 & \text{for } x_i \text{ in } BI \cup cBI \\ 0 & \text{for } x_i = 0 \\ -1 & \text{for } x_i \text{ in } c^2BI \cup c^3BI \end{cases}$$

Example 4. Let $\underline{x}$ be the maximal linearly recurring sequence of Example 1 for $\theta^2 + \theta + 2$ over GF(5). The associated $OC^{(2)}$ sequence $\underline{s}^{(2)}$ is the image of $\underline{x}$ under the mapping

$$\begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 \\ + \\ + \\ - \\ - \end{bmatrix}$$

The primitive root is 2 and the set BI consists only of the element 1,

$$\underline{s}^{(2)} = (0 + - - - - 0 + - - + - 0 - + + + + 0 - + + - +),$$

$$\underline{S}^{(2)} = (20, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,$$

$$-20, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

The pair $\underline{s}$ and $\underline{s}^{(2)}$ of Example 4 are orthogonal (zero cross-correlation). However, the effective auto-correlation periods of $\underline{s}$ and $\underline{s}^{(2)}$ are 6 and 12, respectively. In this case there is no third sequence $\underline{s}^{(\frac{1}{2})}$, since $Q/2 = 12/2 = 6$ is even.

The smallest value of Q for which a complete orthogonal triple $\underline{s}^{(2)}$, $\underline{s}$, $\underline{s}^{(\frac{1}{2})}$ exists is 62. In this case $q = 5$, and $m = 3$. The sequences $\underline{s}^{(2)}$, $\underline{s}$, and $\underline{s}^{(\frac{1}{2})}$ have periods 124, 62, and 31, respectively. With respect to auto-correlation, the effective periods (distances between peaks) for $\underline{s}^{(2)}$, $\underline{s}$, and $\underline{s}^{(\frac{1}{2})}$ are 62, 31, and 31, respectively. All three sequences are derived, by the methods described above, from the maximal linearly recurring sequence for the polynomial $\theta^3 + 4\theta + 3$ over GF(5).

The ternary sequences of types $OC^{(\frac{1}{2})}$, OC, $OC^{(2)}$ all consist of 0, 1's, and -1's. For each such sequence $\underline{s}$ the associated radar signal is defined by

$$F(t) = s_k \sin(2\pi f_c t) = \begin{cases} \sin(2\pi f_c t) & \text{for } s_k = 1 \\ 0 & \text{for } s_k = 0 \\ \sin(2\pi f_c t + \pi) & \text{for } s_k = -1 \end{cases}$$

in the time interval $k \leq t < k + 1$. The periods of the three types $OC^{(\frac{1}{2})}$, OC, $OC^{(2)}$ are $\frac{1}{2}Q$, Q, $2Q$, respectively. For each type the ratio

$$\frac{\text{number of zeros}}{\text{period}}$$

is $(q^{m-1}-1)/(q^m-1) \approx q^{-1}$, which is a measure of power loss due to shutdown intervals.

Table 1 gives conditions on q and m necessary for the three types of ternary sequences. Only when $q \equiv 1 \pmod 4$ and m is odd does one obtain the complete orthogonal triple. When $q \equiv 3 \pmod 4$ and m is even, only the OC sequence exists. In the remaining cases either the orthogonal pair $OC^{(\frac{1}{2})}$, OC or the orthogonal pair OC, $OC^{(2)}$ exists.

Table 2 lists the pairs (q, m) with OC period $2(q^m-1)/(q^m-1) < 20000$, $q < 100$, and $m \geq 3$. This list does not include over 1200 additional cases with $100 < q < 10000$ and $m = 2$. For each such exclusion there is an OC sequence of period $2q + 2$. For roughly one-half of the excluded cases (those for which $q \equiv 1 \pmod 4$) there is also an $OC^{(2)}$ sequence of period $4q + 4$.

Primitive trinomials of degree m, $2 \leq m \leq 10$, are listed in Table 3.

TABLE 1. Requirements for Ternary Sequences.

Conditions on q, m	Type	Period	Peak separation
$q \equiv 3 \pmod 4$ m even	OC	2M	M
$q \equiv 1 \pmod 4$ m even	$OC^{(2)}$ OC	4M 2M	2M M
$q \equiv 3 \pmod 4$ m odd	OC $OC^{(1/2)}$	2M M	M M
$q \equiv 1 \pmod 4$ m odd	$OC^{(2)}$ OC $OC^{(1/2)}$	4M 2M M	2M M M

$M = (q^m-1)/(q-1)$

TABLE 2. Sets of Ternary Sequences.

$q < 100$, $m \geq 3$, $(q^m-1)/(q-1) < 10000$.

q	m	Periods			q	m	Periods		
		$OC^{(\frac{1}{2})}$	OC	$OC^{(2)}$			$OC^{(\frac{1}{2})}$	OC	$OC^{(2)}$
3	3	13	26		47	3	2257	4514	
5	3	31	62	124	13	4		4760	9520
3	4		80		49	3	2451	4902	9804
7	3	57	114		7	5	2801	5602	
9	3	91	182	364	53	3	2863	5726	11452
3	5	121	242		3	8		6560	
11	3	133	266		59	3	3541	7082	
5	4		312	624	61	3	3783	7566	15132
13	3	183	366	732	5	6		7812	15624
17	3	307	614	1228	67	3	4557	9114	
3	6		728		71	3	5113	10226	
19	3	381	762		17	4		10440	20880
7	4		800		73	3	5403	10806	21612
23	3	553	1106		79	3	6321	12642	
25	3	651	1302	2604	83	3	6973	13946	
27	3	757	1514		19	4		14480	
5	5	781	1562	3124	9	5	7381	14762	29524
9	4		1640	3280	89	3	8011	16022	32044
29	3	871	1742	3484	97	3	9507	19014	38028
31	3	993	1986		3	9	9841	19682	
3	7	1093	2186						
37	3	1407	2814	5628					
11	4		2928						
41	3	1723	3446	6892					
43	3	1893	3786						

TABLE 3. Primitive Trinomials Over GF(3).

Degree $\leq$ 13.

Degree	T(θ)	Period
2	$\theta^2 - \theta - 1$	8
3	$\theta^3 - \theta + 1$	26
4	$\theta^4 - \theta - 1$	80
5	$\theta^5 - \theta + 1$	242
6	$\theta^6 - \theta - 1$	728
7	$\theta^7 - \theta^2 + 1$	2186
8	$\theta^8 - \theta^3 - 1$	6560
9	$\theta^9 - \theta^4 + 1$	19 682
10	None	
11	$\theta^{11} - \theta^2 + 1$	177 146
	$\theta^{11} - \theta^3 + 1$	177 146
12	None	
13	$\theta^{13} - \theta + 1$	1 594 322
	$\theta^{13} - \theta^4 + 1$	1 594 322
	$\theta^{13} - \theta^6 + 1$	1 594 322

$T(-\theta)$ primitive for even degree.

$T(\theta^{-1})$ primitive for all degrees.

3. POLYPHASE PN CODES

Another type of phase modulated spread spectrum signal can be formed by associating the p distinct members $0, 1, 2, \ldots, p-1$ of the finite field GF(p) with the equally spaced phases $0, 2\pi/p, 4\pi/p, \ldots, 2(p-1)\pi/p$. Given a linearly recurring sequence $\underline{x}$ over GF(p), the transmitted signal during the k^{th} time interval (bit) is $\sin[2\pi f_o t + (2\pi x_k)/p]$. It is mathematically expedient to represent the k^{th} bit by ω^{x_k}, where $\omega = e^{2\pi i/p}$, a primitive p^{th} root of 1.

Example 5. For $p = 5$, the MLRS determined by the primitive quadratic $\theta^2 + \theta + 2$ is

$$\underline{x} = (0\ 1\ 4\ 4\ 3\ 4\ 0\ 2\ 3\ 3\ 1\ 3\ 0\ 4\ 1\ 1\ 2\ 1\ 0\ 3\ 2\ 2\ 4\ 2)$$

The corresponding sequence of phases is

$$(0°, 72°, 288°, 288°, 216°, 288°, 0°, 144°, \ldots)$$

This sequence $\underline{x}$ over GF(5) is the same as the one used in Example 1 to determine a ternary OC sequence with period 12.

When used to form a polyphase signal an MLRS over GF(p) is called a p-ary PN code. The analogy between such sequences and the usual binary PN codes is obvious. Rather than a pseudo-random hop between the two phases $0, \pi$ induced by a binary PN code, the p-ary PN code induces a pseudo-random hop among the p phases $0, 2\pi/p, \ldots, 2(p-1)\pi/p$. For each odd prime p and positive integer m, distinct polynomials which are primitive of degree m over GF(p) determine cyclically inequivalent p-ary PN codes. With slight modification the algebraic theory underlying binary PN codes applies to p-ary PN codes.

The p-ary PN codes of degree m have period $L = p^m - 1$. The autocorrelation coefficient is

$$c_\tau = \sum_{k=0}^{L-1} \omega^{x_k} \overline{\omega}^{x_{k+\tau}}$$

where $\overline{\omega}$ is the complex conjugate of ω. The p-ary PN codes admit the generalized shift and add property

$$x_k + \alpha x_{k+\tau} = x_{k+\sigma} \qquad 0 \leq k \leq L-1$$

whenever α is in GF(p). Applying this with $\alpha = -1$ gives

$$x_k - x_{k+\tau} = x_{k+\sigma}$$

and

$$c_\tau = \sum_{k=0}^{L-1} \omega^{x_k - x_{k+\tau}} = \sum_{k=0}^{L-1} \omega^{x_\sigma}$$

The frequencies of occurrences of members of GF(p) in an MLRS are given by

$$x_k = \beta \quad \begin{cases} \text{for } p^{m-1} \text{ values of } k \text{ if } \beta \neq 0 \\ \text{for } p^{m-1}-1 \text{ values of } k \text{ if } \beta = 0 \end{cases}$$

This accounts for all $p^m - 1$ values of k and establishes

$$c_\tau = \begin{cases} L & \text{for } \tau = 0 \\ -1 & \text{otherwise} \end{cases}$$

Example 6. The difference between $\underline{x}$ and its first shift in Example 5 is the 22^{nd} shift of $\underline{x}$.

$$\begin{array}{l} (0\ 1\ 4\ 4\ 3\ 4\ 0\ 2\ 3\ 3\ 1\ 3\ 0\ 4\ 1\ 1\ 2\ 1\ 0\ 3\ 2\ 2\ 4\ 2) \\ -(1\ 4\ 4\ 3\ 4\ 0\ 2\ 3\ 3\ 1\ 3\ 0\ 4\ 1\ 1\ 2\ 1\ 0\ 3\ 2\ 2\ 4\ 2\ 0) \\ \hline (4\ 2\ 0\ 1\ 4\ 4\ 3\ 4\ 0\ 2\ 3\ 3\ 1\ 3\ 0\ 4\ 1\ 1\ 2\ 1\ 0\ 3\ 2\ 2) \end{array}$$

For $m = 1$, the p-ary PN code $\underline{x}$ has period $p-1$ and is generated by some linear polynomial $\theta - \gamma$, where γ is a primitive root in GF(p).[6] For some large values of p, roots γ (called multipliers) are judiciously selected to produce sequences of pseudo-random uniform numbers

$$\gamma^a/p,\ \gamma^{a+1}/p,\ \gamma^{a+2}/p,\ \ldots\ ,$$

for digital computer simulations.[7]

It should be emphasized that whereas every pair (q, m), $q = p^r$, yields a ternary sequence of period $2(q^m-1)/(q-1)$, perhaps two or three such sequences, only for the cases $q = p$ $(r = 1)$, do the p-ary phase hop codes exist. The MLRS's over GF(q), with $q > p$, do not lend themselves so easily to polyphase signal design. This stems from the fundamental algebraic operations within GF(q). A group of equally spaced phases corresponding to the p^{th} roots of unity $1, \omega, \omega^2, \ldots, \omega^{p-1}$ is cyclic under the multiplicative operation. But the additive group of

GF(q) is cyclic only for $q = p$, $r = 1$. The ternary sequences of Section 2 are based upon multiplication in GF(q), not addition. The multiplicative group of non-zero elements in every finite field is cyclic.

This problem also arises when one attempts to construct polyphase signals from MLRS's over $GF(2^r)$. What is required is an appropriate mapping from the field elements, considered additively, to some set of complex roots of unity. Such mappings probably exist, but there is no obvious one, since no group isomorphism exists. For the field GF(4), some interesting quadriphase signals have been studied.[9]

4. SPECTRAL PROPERTIES OF TERNARY SEQUENCES

By the spectrum of a sequence $\underline{s} = (s_0, s_1, \ldots, s_{n-1})$ is meant the sequence $\underline{a} = (a_0, a_1, \ldots a_{N-1})$ of non-negative real numbers defined by

$$a_k = \left| \sum_{t=0}^{N-1} s_t \omega^{kt} \right|, \qquad 0 \leq k < N$$

where $\omega = e^{2\pi i/N}$. The plots of a_k against k are scaled. For Figures 3, 4, and 5, the scaling reduces the maximum a_k to 1.0. Figures 6 through 9 are scaled by the same factor as Figure 4, while Figures 10 through 13 are scaled by the same factor as Figure 5.

Figures 3, 4, and 5 show the spectra of a 15-bit binary PN sequence, the OC sequence $\underline{s}$ of Example 3, and the $OC^{(\frac{1}{2})}$ sequence $\underline{s}^{(\frac{1}{2})}$ of Example 3, respectively. The $(\sin k)/k$ shape of the enclosing envelope apparent for each of the three spectra occurs because of the impulse-like auto-correlation of each sequence. For the OC sequence $\underline{s}$ of Figure 4, spectral lines occur only at the odd multiples of the word frequency f_w. This follows from the negacyclic property of $\underline{s}$; namely $s_{t+13} = -s_t$, all t, while the period of $\underline{s}$ is 26.

---

[9] Rockwell International Corporation, Collins Radio Group. *Study of Multi-State PN Sequences and Their Application to Communication Systems*, by Robert Gold. Prepared for Naval Research Laboratories, July, 1976, Final Report. Publication UNCLASSIFIED.

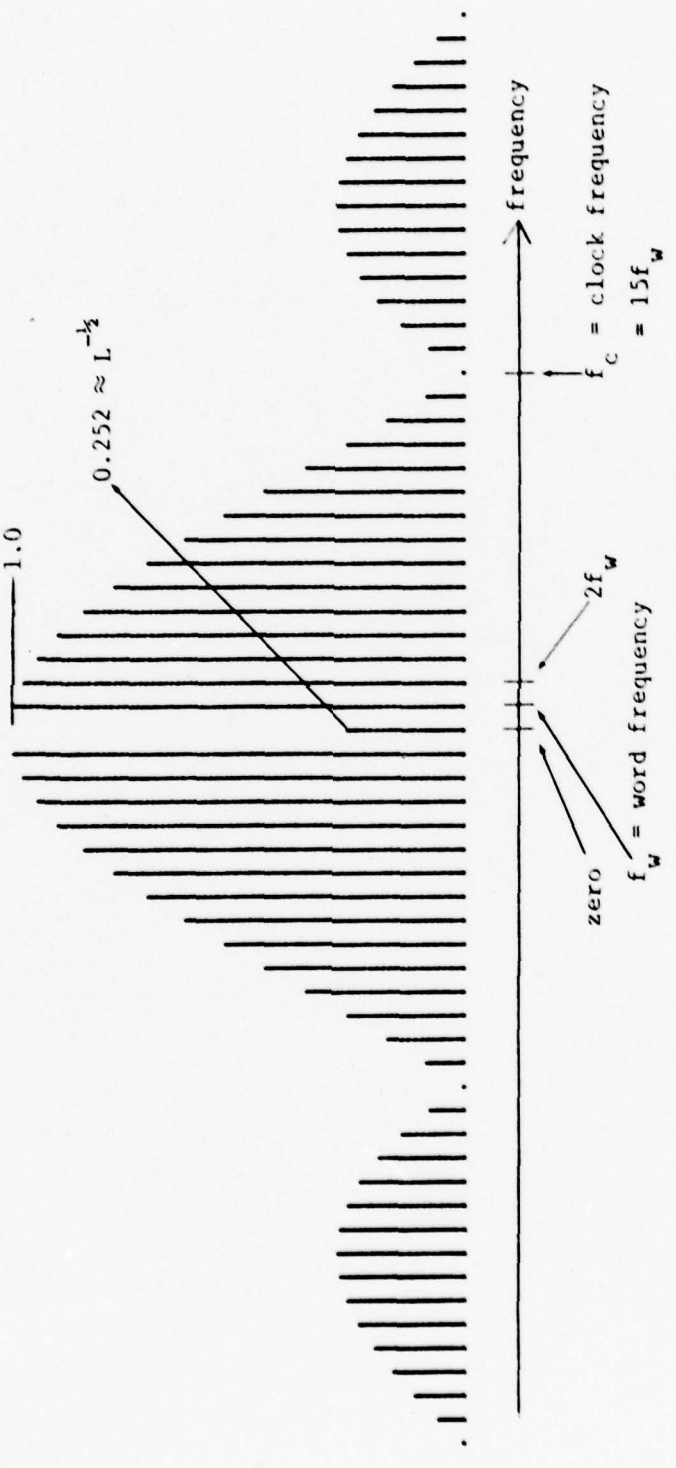


FIGURE 3. Spectrum of 15-Bit Binary PN Code. (Four samples per bit.)

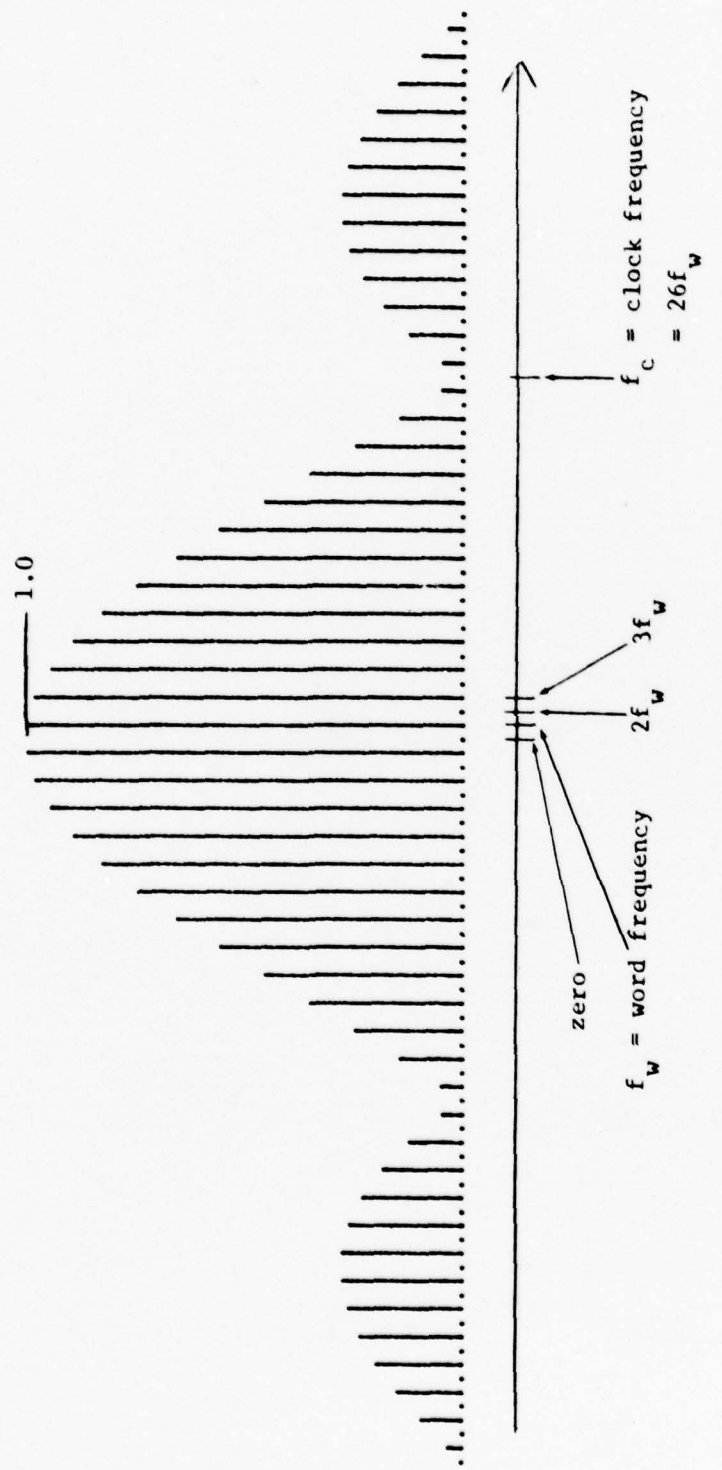


FIGURE 4. Spectrum of 26-Bit OC Sequence.
(Four samples per bit.)

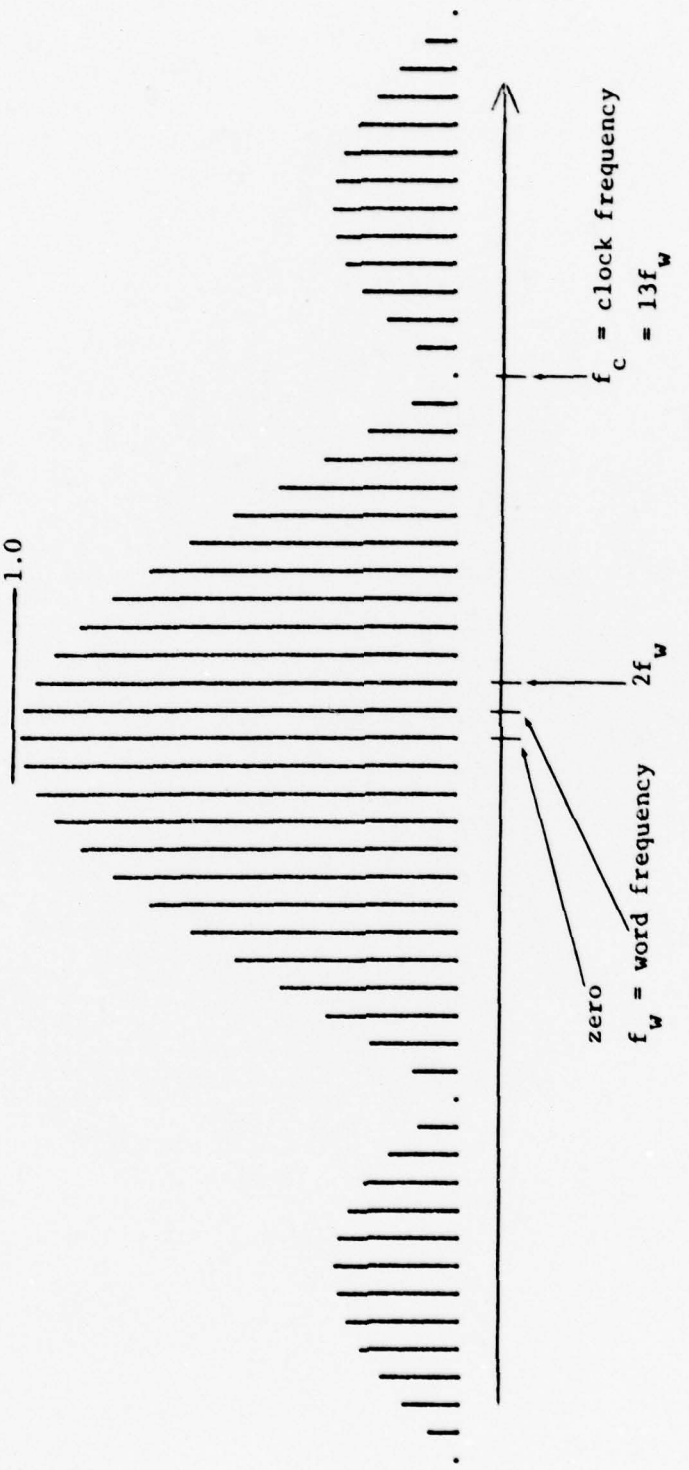


FIGURE 5. Spectrum of 13-Bit OC($\frac{1}{2}$) Sequence.
(Four samples per bit.)

Since the auto-correlation of $\underline{s}$ has two spikes per period, the first range ambiguity corresponds to the frequency $2f_w$ rather than to f_w. The presence of the spectral line at f_w could be a disadvantage in some applications where the product (mixed) code $\underline{s} \cdot \underline{s}_\tau$ is low pass filtered. However, the negacyclic property of $\underline{s}$ guarantees that $\underline{s} \cdot \underline{s}_\tau$ has period one-half the period of $\underline{s}$. Thus, the spectrum of $\underline{s} \cdot \underline{s}_\tau$ has no lines at odd multiples of f_w. This is shown in Figures 6 through 9 corresponding to the four product sequences $\underline{s} \cdot \underline{s}_\tau$, $1 \leq \tau \leq 4$. These represent shifts $\underline{s}_\tau$ through an integer number of bits.

The comparatively large line at zero frequency for the $OC^{(\frac{1}{2})}$ sequence $\underline{s}^{(\frac{1}{2})}$ arises from the excess of +1's over -1's in the sequence. This line could also cause serious problems when filtering the product sequence $\underline{s}^{(\frac{1}{2})} \cdot \underline{s}_\tau^{(\frac{1}{2})}$. But the zero side lobes in the auto-correlation of $\underline{s}^{(\frac{1}{2})}$ force the zero spectral line to zero when $\tau \neq 0$. This can be seen in Figures 10 through 13 for the products $\underline{s}^{(\frac{1}{2})} \cdot \underline{s}_\tau^{(\frac{1}{2})}$, $1 \leq \tau \leq 4$.

For a binary PN sequence $\underline{x}$, the shift and add property guarantees that $\underline{x} \cdot \underline{x}_\tau$ is a PN sequence. Thus, the spectrum of $\underline{x} \cdot \underline{x}_\tau$ also possesses a $(\sin k)/k$ envelope for τ a non-zero integer. Since none of the OC sequences has the shift and add property, the spectra of the product sequences vary considerably.

The p-ary PN sequences described in Section 3 do satisfy the shift and add condition. This together with their impulse-like auto-correlations guarantee the $(\sin k)/k$ envelope for the products corresponding to integer shifts.

As with binary PN codes, the ternary and polyphase codes would require more detailed analysis and computation regarding their ambiguity functions in order to determine their suitability for particular applications.

5. SHIFT REGISTERS OVER GF(q)

Any linearly recurring sequence $\underline{x}$ defined by a polynomial $f(\theta)$ over GF(q) can "formally" be generated by a (linear feed-back) shift register.[3] Figure 14 shows a shift register for the quartic $x^4 - ax - b$ over GF(q). Over GF(2) linear shift registers require no multipliers, since 1 is the only non-zero element. Multiplication by 1 simply amounts to a delay. However, in GF(q) there are $q - 2$ non-zero elements different from 1. The implementation of a shift register such as the one in Figure 14 would require devices to multiply by a and by b in GF(q), a GF(q) adder, and q-state devices to represent the elements x_{k-j}.

Efficient, high-speed devices for the elements and operations in GF(q) are not currently available. Clearly a set of R binary flip-flops can

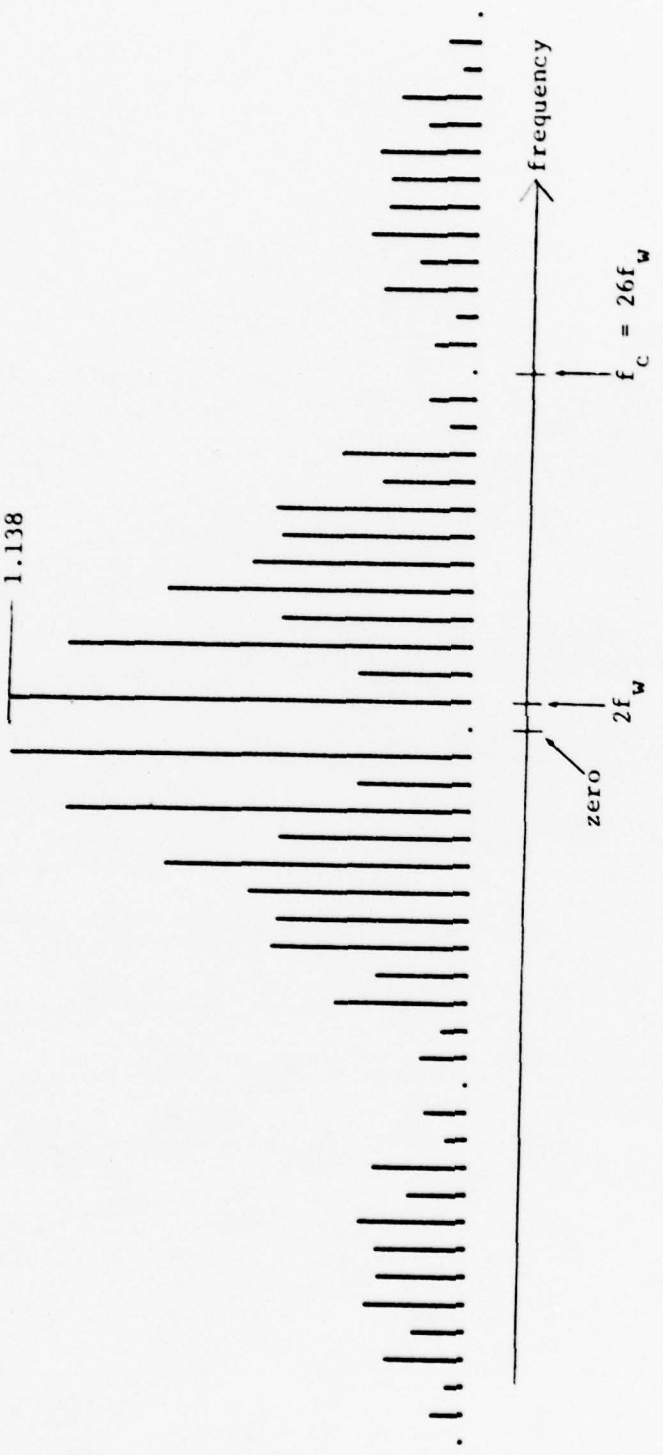


FIGURE 6. Spectrum of $\underline{s} \cdot \underline{s}_1$, QC Product.
(Four samples per bit.)

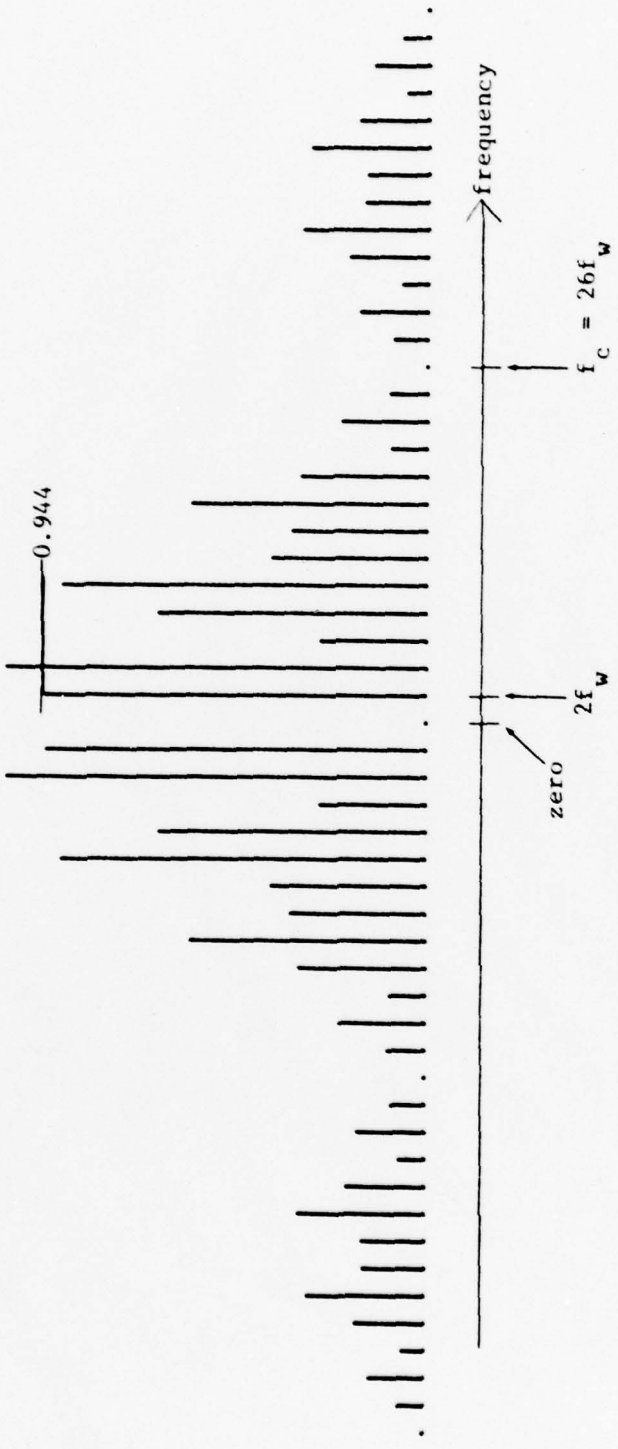


FIGURE 7. Spectrum of $\underline{s} \cdot \underline{s}_2$, OC Product. (Four samples per bit.)

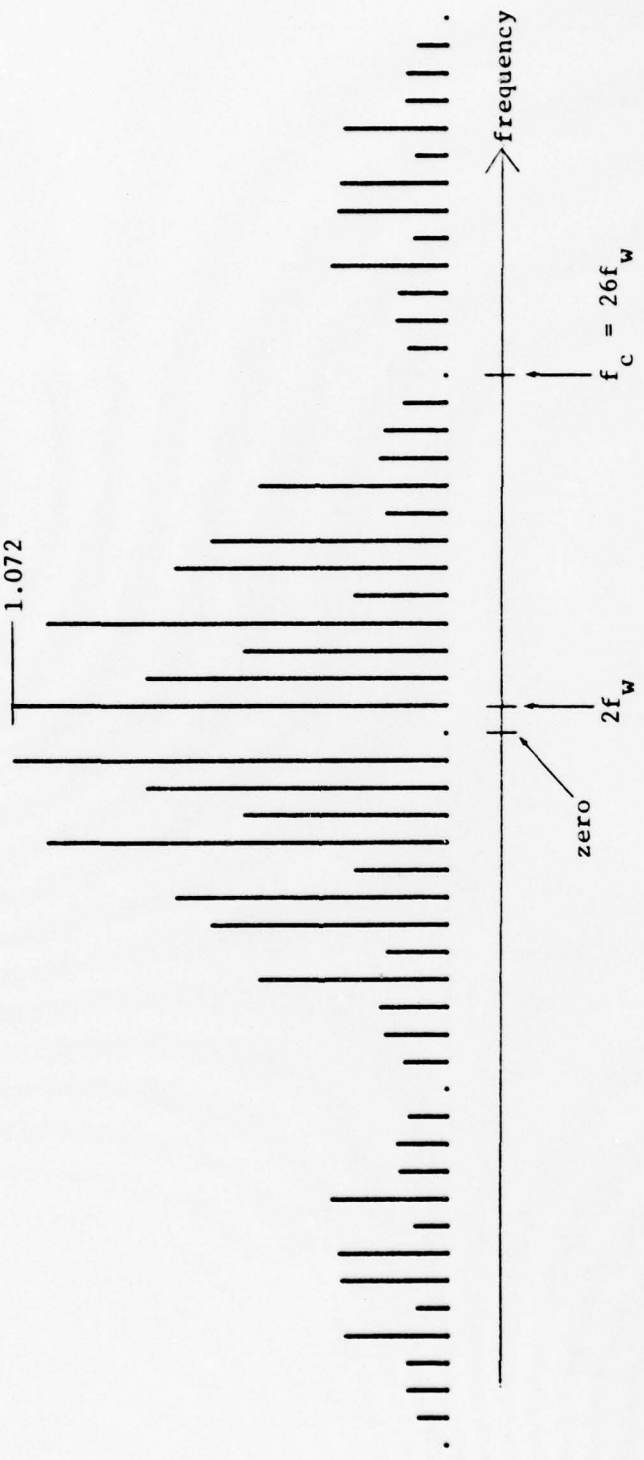


FIGURE 8. Spectrum of $\underline{s} \cdot \underline{s}_3$, OC Product.
(Four samples per bit.)

26

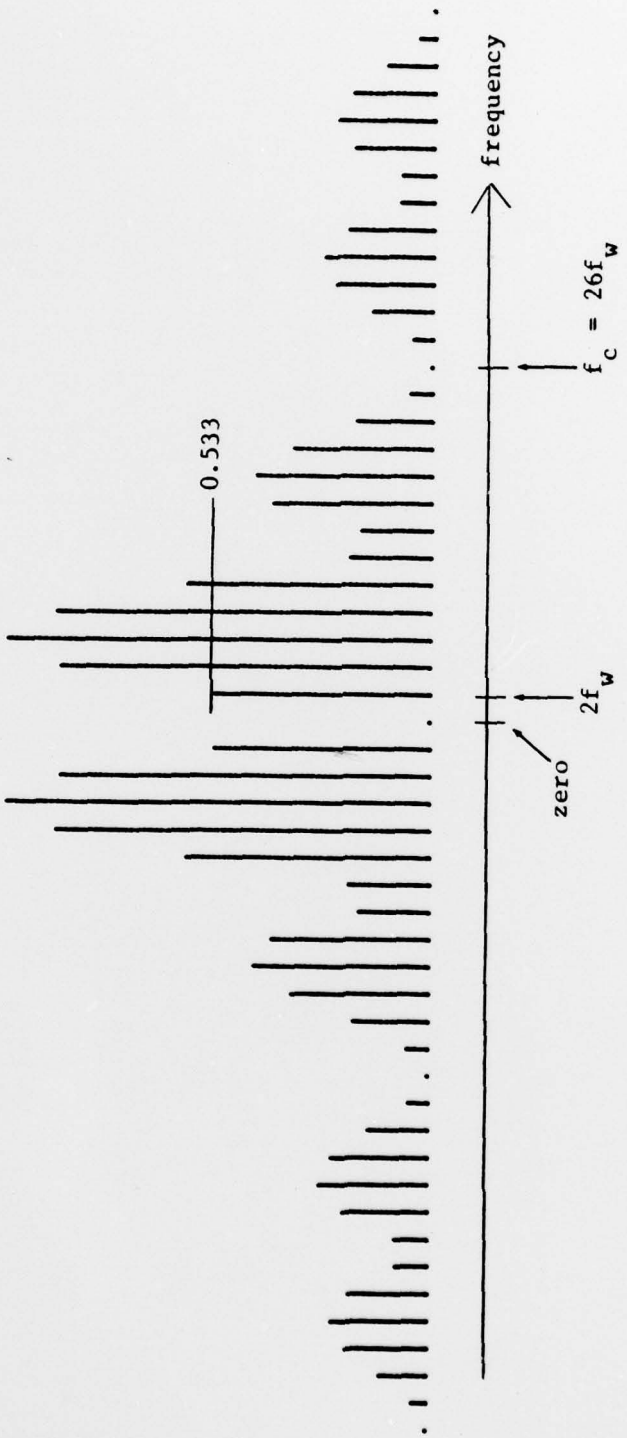


FIGURE 9. Spectrum of $\underline{s} \cdot \underline{s}_4$, OC Product.
(Four samples per bit.)

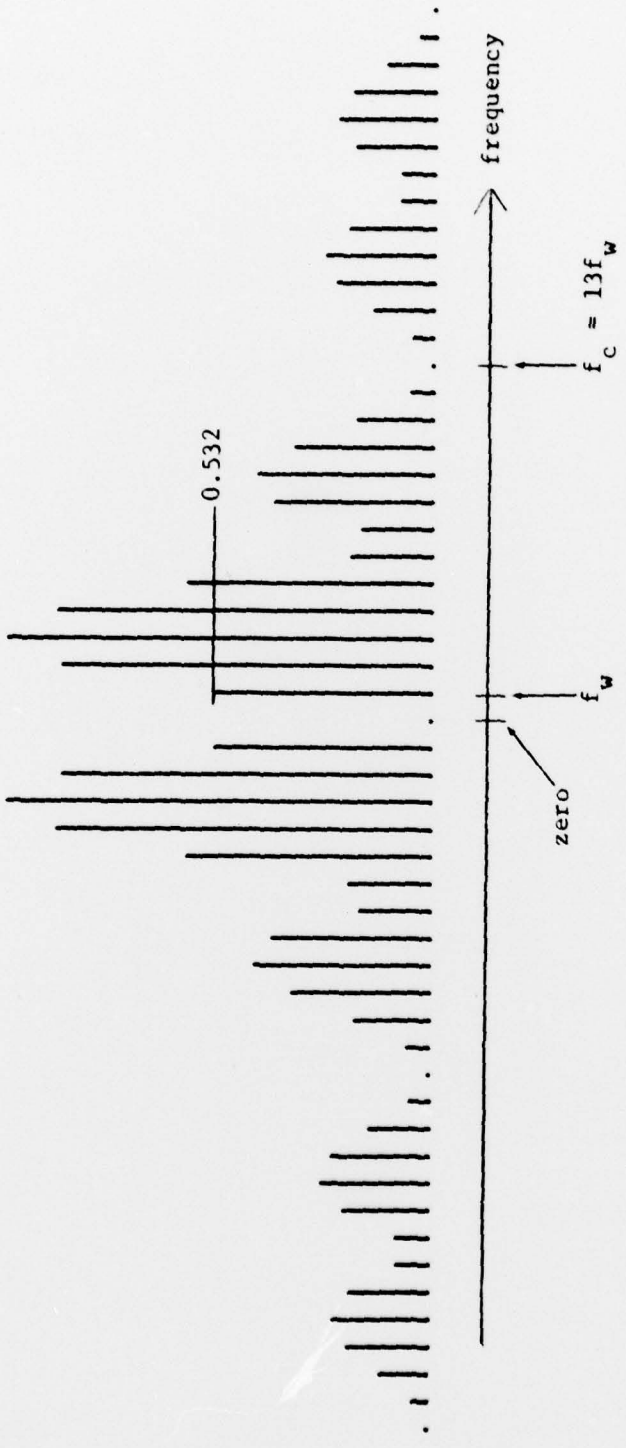


FIGURE 10. Spectrum of $\underline{s}^{(\frac{1}{2})} \cdot \underline{s}_1^{(\frac{1}{2})}$, $OC^{(\frac{1}{2})}$ Product.
(Four samples per bit.)

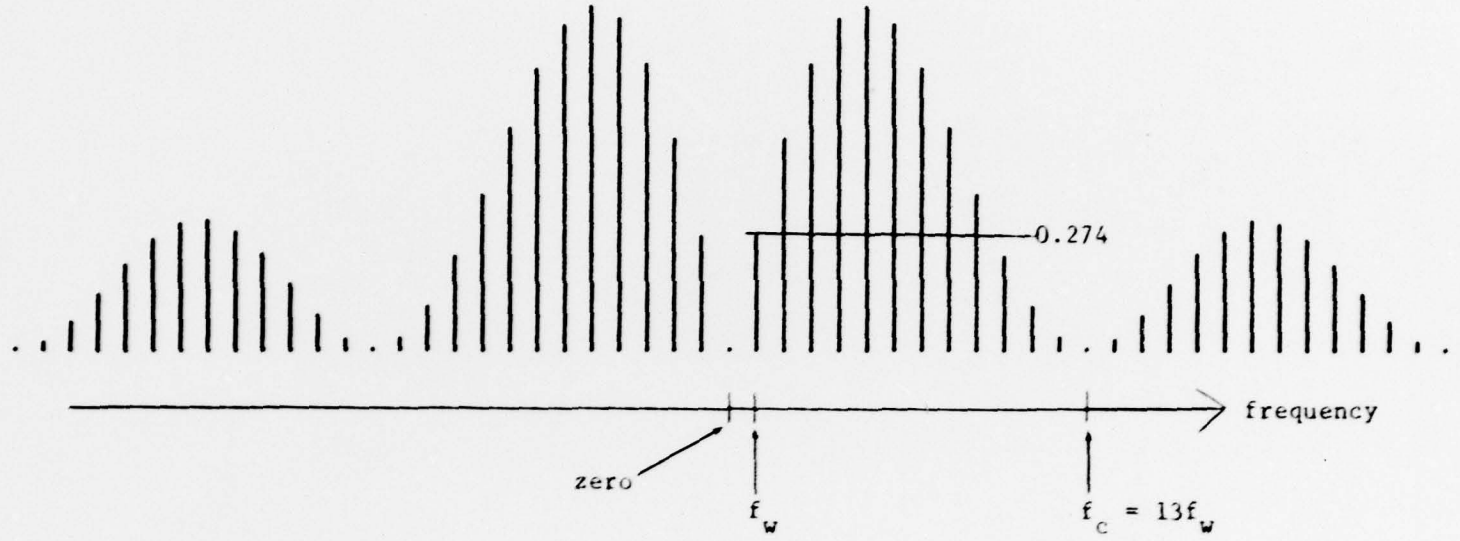


FIGURE 11. Spectrum of $\underline{s}^{(\frac{1}{2})} \cdot \underline{s}_2^{(\frac{1}{2})}$, $OC^{(\frac{1}{2})}$ Product.
(Four samples per bit.)

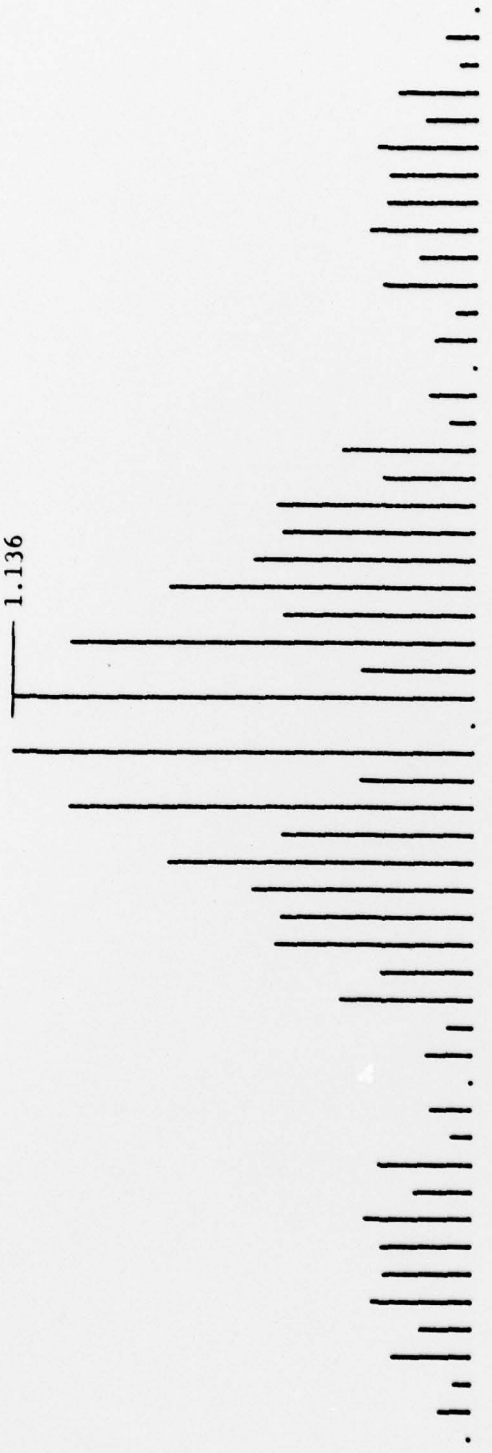


FIGURE 12. Spectrum of $\underline{s}^{(\frac{1}{2})} \cdot \underline{s}_3^{(\frac{1}{2})}$, $OC^{(\frac{1}{2})}$ Product.
(Four samples per bit.)

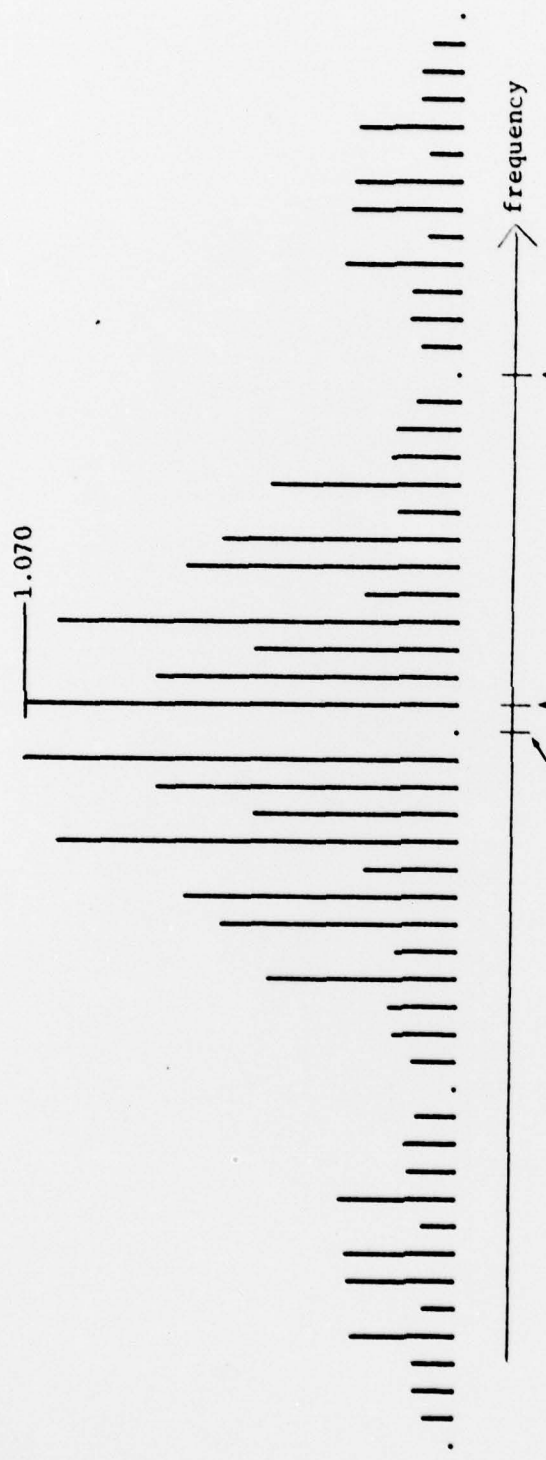
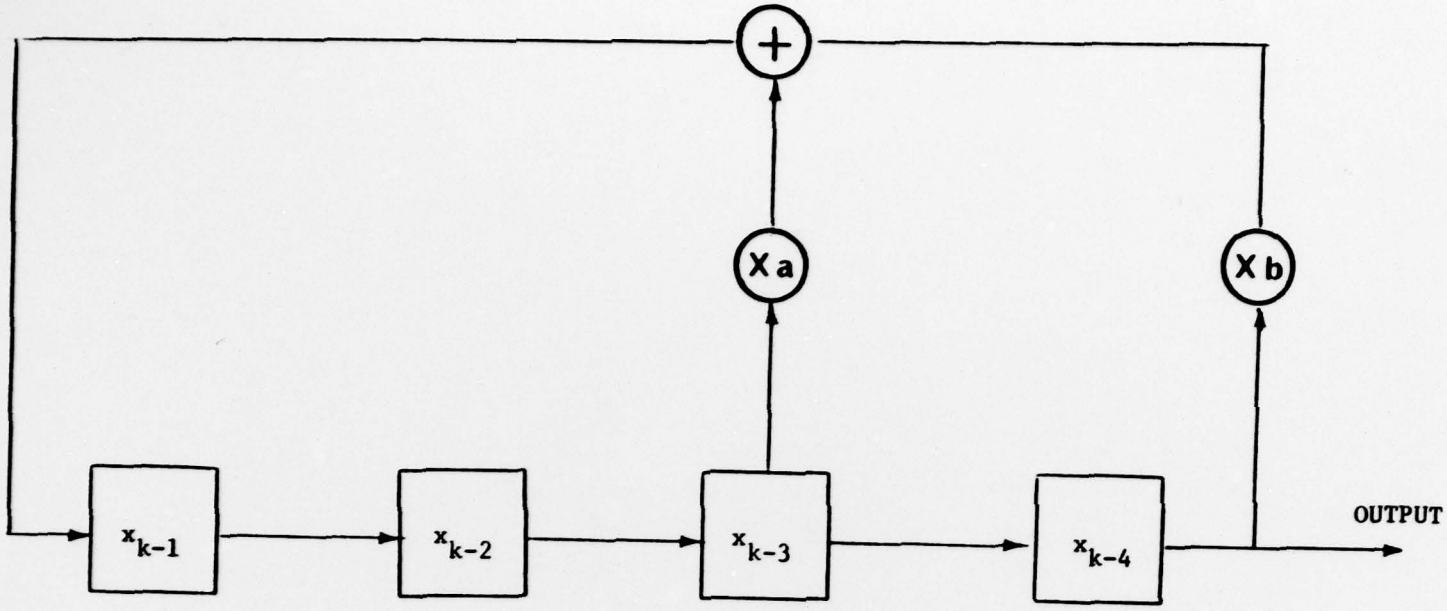


FIGURE 13. Spectrum of $s^{(\frac{1}{2})} \cdot s^{(\frac{1}{2})}$, $OC^{(\frac{1}{2})}$ Product.
(Four samples per bit.)



+ = addition in GF(q)

Xa = multiplication by a in GF(q)

Xb = multiplication by b in GF(q)

FIGURE 14. Shift Register for $f(\theta) = \theta^4 - a\theta - b$ Over GF(q).

32

be configured to represent the q distinct elements of GF(q), provided $2^R \geq q$. A cursory examination of the problem of carrying out addition in GF(3) using binary XOR and AND gates has revealed no simple or elegant solution.

Operating in GF(p) is all that is required to generate the p-phase codes of Section 3. In order to generate the ternary codes of Section 2, one must also implement the mapping

$$\begin{pmatrix} \text{residue} \\ 0 \\ \text{non-residue} \end{pmatrix} \longrightarrow \begin{pmatrix} +1 \\ 0 \\ -1 \end{pmatrix}$$

This requires "recognizing" the quadratic residues in GF(q). Depending upon how the elements of GF(q) are represented, the recognition of quadratic residues could be an even more difficult problem. Of course, for small q, a table look-up is feasible.

The elements of $GF(p^r)$ are usually represented as r-dimensional vectors over GF(p). Even if one has succeeded in dealing with GF(p), the vectors corresponding to the quadratic residues in GF(q) are still difficult to recognize.

It is apparent that the generation of GF(q)-linear sequences is a problem worthy of further investigation.

REFERENCES

1. *Digital Communications with Space Applications*, ed. by S. W. Golomb. New York, Prentice Hall, 1964.

2. S. W. Golomb. *Shift Register Sequences*. San Francisco, Holden-Day, 1967.

3. W. W. Peterson and E. W. Weldon. *Error-correcting Codes*, 2nd ed. Cambridge, The M.I.T. Press, 1972.

4. J. Singer. "A Theorem in Finite Projective Geometry and Some Applications to Number Theory," *Amer. Math. Soc. Trans.*, Vol. 43 (1938), pp. 377-385.

5. M. Hall. "An Isomorphism Between Linear Recurring Sequences and Algebraic Rings," *Amer. Math. Soc., Trans.*, Vol. 44 (1938), pp. 196-218.

6. J. M. Alsup and J. M. Speiser. "Exponential Residue Codes," *IEEE Trans. Aerospace and Elec. Sys.*, November, 1975, pp. 1389-1390.

7. D. E. Knuth. *The Art of Computer Programming*. Vol. 2, Seminumerical Algorithms. Reading, Mass., Addison-Wesley, 1969.

8. J. H. E. Elliott and A. T. Butson. "Relative Difference Sets," *Ill. J. Math.*, Vol. 10 (1966), pp. 517-531.

9. Rockwell International Corporation, Collins Radio Group. *Study of Multi-State PN Sequences and Their Application to Communication Systems*, by Robert Gold. Prepared for Naval Research Laboratories, July, 1976, Final Report. Publication UNCLASSIFIED.

Appendix A

TWO SEQUENCES OVER GF(9)

The elements of GF(3) are 0, the non-zero quadratic residue 1, and the quadratic non-residue $2 = -1$. In order to compute in GF(9), a representation of the elements of GF(9) as 2-dimensional vectors over GF(3) is required. Such a representation requires an irreducible quadratic over GF(3). Since the algebraic relationship between the reducibility of quadratics and the quadratic character of their discriminants (which is used to solve real quadratics) persists in fields of odd characteristic, one needs a quadratic over GF(3) with non-residue discriminant in order to construct GF(9). There are three such quadratics over GF(3).

$$\theta^2 + 1, \qquad \theta^2 + \theta + 2, \qquad \theta^2 + 2\theta + 2$$

Each of these quadratics, irreducible over GF(3), has two roots in GF(9). Indeed, the six elements of GF(9), not in GF(3), are precisely these roots. The roots of $\theta^2 + 1$ are square roots of -1. Hence, their multiplicative order is 4, and they are not primitive. The four primitive roots, each of multiplicative order 8, are the roots of $\theta^2 + \theta + 2$ and $\theta^2 + 2\theta + 2$.

Let γ be one root of $\theta^2 + 2\theta + 2$. Then $\gamma^2 = \gamma + 1$. This relation enables one to express every element in GF(9) in the form $\alpha\gamma + \beta$, where α and β are elements of GF(3). It is, of course, no accident that the pair (α, β) can be selected in exactly nine ways. Thus, one obtains the 1-1 correspondence between the members of GF(9) and the 2-dimensional vectors over GF(3). (Analogously the set of all numbers $\alpha\gamma + \beta$, with α and β rational, form a subfield of the algebraic numbers, when $\gamma = -1 + \sqrt{2}$. Note that $-1 + \sqrt{2}$ is a root of $\theta^2 + 2\theta - 1$, which has no rational roots.)

The representation of GF(9) starting with the root γ of $\theta^2 + 2\theta + 2$ $[= \theta^2 + 2\theta - 1]$ is

$$
\begin{aligned}
0 &= 0\gamma + 0 \longrightarrow (0, 0)\\
\gamma &= 1\gamma + 0 \longrightarrow (1, 0)\\
\gamma^2 &= 1\gamma + 1 \longrightarrow (1, 1)\\
\gamma^3 &= 2\gamma + 1 \longrightarrow (2, 1)\\
\gamma^4 &= 0\gamma + 2 \longrightarrow (0, 2)\\
\gamma^5 &= 2\gamma + 0 \longrightarrow (2, 0)\\
\gamma^6 &= 2\gamma + 2 \longrightarrow (2, 2)\\
\gamma^7 &= 1\gamma + 2 \longrightarrow (1, 2)\\
1 = \gamma^8 &= 0\gamma + 1 \longrightarrow (0, 1)
\end{aligned}
$$

Addition in GF(9) is coordinate-wise addition modulo 3. Multiplication in GF(9) can be accomplished by determining the powers of γ corresponding to (α_1, β_1) and (α_2, β_2), and then adding the exponents modulo 8. For example

$$
\begin{aligned}
(2,1)(1,2) &\longrightarrow (2\gamma + 1)(\gamma + 2)\\
&= 2\gamma^2 + 5\gamma + 2\\
&= 7\gamma + 4\\
&= \gamma + 1 \longrightarrow (1,1)
\end{aligned}
$$

In order to construct the OC and $OC^{(2)}$ sequences for $q = 9$, $m = 2$, one needs a primitive quadratic over GF(9). This requires finding quadratics over GF(9) with discriminants which are quadratic non-residues in GF(9). The non-residues in GF(9) are γ, γ^3, γ^5, and γ^7. (It should be observed here that the two quadratics, which are primitive over GF(3), factor over GF(9). Namely $\theta^2 + 2\theta + 2 = (\theta - \gamma)(\theta - \gamma^3)$ and $\theta^2 + \theta + 2 = (\theta - \gamma^5)(\theta - \gamma^7)$.) Among the quadratics irreducible over GF(9), some are primitive, some are not. Recall that although $\theta^2 + 1$ is irreducible over GF(3), it is not primitive. Over GF(9), the quadratic $\theta^2 + 2\theta + 2\gamma^2$ is irreducible, but not primitive; it is irreducible because its discriminant, γ^7, is a non-residue. The quadratic $\theta^2 + 2\gamma\theta + 2\gamma$ is primitive and can be used to define an MLRS of period 80 over GF(9). The first 40 members of the MLRS $\underline{x}$ are

$$
\begin{aligned}
(&0\ \ 1\ \ \gamma\ \ \gamma^3\ \ \gamma\ \ \gamma\ \ \gamma^6\ \ \gamma^5\ \ 1\ \ \gamma^4\\
&0\ \ \gamma^5\ \ \gamma^6\ \ 1\ \ \gamma^6\ \ \gamma^6\ \ \gamma^3\ \ \gamma^2\ \ \gamma^5\ \ \gamma\\
&0\ \ \gamma^2\ \ \gamma^3\ \ \gamma^5\ \ \gamma^3\ \ \gamma^3\ \ 1\ \ \gamma^7\ \ \gamma^2\ \ \gamma^6\\
&0\ \ \gamma^7\ \ 1\ \ \gamma^2\ \ 1\ \ 1\ \ \gamma^5\ \ \gamma^4\ \ \gamma^7\ \ \gamma^3)
\end{aligned}
$$

The remaining 40 members of one period of $\underline{x}$ are the negatives of the first 40 members.

To obtain the OC, and $OC^{(2)}$ sequences from $\underline{x}$ the following mappings are used

OC

$$\begin{bmatrix} 0 \\ 1 \\ \gamma \\ \gamma^2 \\ \gamma^3 \\ \gamma^4 \\ \gamma^5 \\ \gamma^6 \\ \gamma^7 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 \\ + \\ - \\ + \\ - \\ + \\ - \\ + \\ - \end{bmatrix}$$

$OC^{(2)}$

$$\begin{bmatrix} 0 \\ 1 \\ \gamma \\ \gamma^2 \\ \gamma^3 \\ \gamma^4 \\ \gamma^5 \\ \gamma^6 \\ \gamma^7 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 \\ + \\ + \\ - \\ - \\ + \\ + \\ - \\ - \end{bmatrix}$$

The resulting sequences are

$$\underline{s} = (0\ +\ -\ -\ -\ -\ +\ -\ +\ +\ 0\ -\ +\ +\ +\ +\ -\ +\ -\ -)$$

$$\underline{s}^{(2)} = (0\ +\ +\ -\ +\ +\ -\ +\ +\ +\ 0\ +\ -\ +\ -\ -\ -\ -\ +\ +$$
$$0\ -\ -\ +\ -\ -\ +\ -\ -\ -\ 0\ -\ +\ -\ +\ +\ +\ +\ -\ -)$$

Appendix B

TRINOMIALS OVER GF(3)

The general trinomial over GF(3) has the form

$$T(\theta) = \theta^m - a\theta^k - b$$

where $1 \leq k \leq m-1$, $a = \pm 1$, and $b = \pm 1$. In order for $T(\theta)$ to be primitive, $T(\theta)$ must be irreducible. In particular, neither linear factor $\theta-1$ or $\theta+1$ can divide $T(\theta)$. Equivalently, $T(\theta)$ must have no roots in GF(3). This eliminates the following cases.

$$\theta^m + \theta^k + 1, \quad \text{all } m \text{ and } k \longrightarrow T(1) = 0$$

$$\left.\begin{array}{ll} \theta^m - \theta^k + 1, & m \text{ even}, \ k \text{ odd} \\ \theta^m - \theta^k - 1, & m \text{ odd}, \ k \text{ even} \\ \theta^m + \theta^k - 1, & m \text{ odd}, \ k \text{ odd} \end{array}\right\} \longrightarrow T(-1) = 0$$

Next consider the companion matrix A for $T(\theta)$

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ & & \vdots & & \vdots & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ & & \vdots & & \vdots & \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ b & 0 & 0 & \cdots & a & 0 \end{bmatrix} \leftarrow \text{Row } k$$

$\uparrow$

Column k+1

If $T(\theta)$ is primitive, then the matrix algebra over GF(3) generated by A is isomorphic to $GF(3^m)$, and A is a root of $T(\theta)$. The mapping $X \longrightarrow \det(X)$ is a homomorphism from the multiplicative group $\langle A \rangle$ onto $\{1,-1\}$, the group of order 2. Since A is a generator of $\langle A \rangle$, $\det(A)$ must generate $\{1,-1\}$. Thus, $\det(A) = -1$.

Since

$$\det(A) = (-1)^{m+1} b$$

it follows that for $T(\theta)$ to be primitive, b must equal $(-1)^m$. This leaves the following possibilities for primitive trinomials.

$$\left.\begin{aligned} &\theta^m - \theta^k - 1 \\ &\theta^m + \theta^k - 1 \end{aligned}\right\} \quad \text{for } m \text{ even}$$

$$\theta^m - \theta^k + 1 \quad \text{for } m \text{ odd}$$

The inverse trinomial

$$\begin{aligned} T^{-1}(\theta) &= -b\theta^m T(\theta^{-1}) \\ &= \theta^m + ab\theta^{m-k} - b \end{aligned}$$

is primitive if and only if $T(\theta)$ is primitive. Therefore, only those trinomials with $2k \leq m$ need be considered. This leaves m, cases for $m = 2m_1 + 1$, and $m/2$ case for m even.

Suppose, however, that the greatest common divisor d of m and k is greater than 1. If α is a root of $T(\theta)$, then $\beta = \alpha^d$ is a root of $U(\theta) = \theta^{m/d} - a\theta^{k/d} - b$. Thus, β has order at most $3^{m/d} - 1$, so the order of α is at most $d(3^{m/d} - 1)$. It follows that α is not primitive of degree m, since

$$d(3^{m/d} - 1) < 3^m - 1 \quad \text{for } 1 < d < m$$

This rules out all cases with m and k not relatively prime. In particular, for m even, k must be odd.

Finally, consider the case m even k odd. Here $T(-\theta) = \theta^m + a\theta^k - b$. If α is a root of $T(\theta)$, and $T(\theta)$ is primitive, then $\alpha^{(3^m-1)/2} = -1$. Since m is even, $(3^m-1)/2$ is also even. Therefore, $-\alpha$ is another primitive root, and $T(-\theta)$ is primitive. It follows that $T(\theta)$ is

primitive if and only if $T(-\theta)$ is primitive when m is even. Only the cases $T(\theta) = \theta^m - \theta^k - 1$ need be considered for m even.

Summary. Every primitive trinomial over GF(3) is obtainable from one of the following two types by one of the transformations $\theta \longrightarrow \theta^{-1}$ or $\theta \longrightarrow -\theta$:

$\theta^m - \theta^k - 1$ for m even, k odd

$\theta^m - \theta^k + 1$ for m odd

This leaves at most $m/4$ or $m/2$ cases to investigate for m even or m odd, respectively.

The irreducibility of $T(\theta)$ can be tested by computing the rank of each matrix

$$D_e = A^{(3^e)} - A, \qquad 1 \leqslant e \leqslant m/2$$

A generates $GF(3^m)$, and $T(\theta)$ is irreducible, if and only if each D_e has full rank m. For any e, deficiency in the rank of D_e indicates that $T(\theta)$ possesses roots in $GF(3^e)$.

The primitivity of irreducible trinomials becomes difficult to establish for large m. For $m \leqslant 13$, a linear recurring sequence defined by $T(\theta)$ can be checked.