USCEE Report 393

UNIVERSITY OF SOUTHERN CALIFORNIA

ON THE CROSS-CORRELATION FUNCTIONS OF MAXIMAL LINEAR RECURRING SEQUENCES

Herbert Mitchell Trachtenberg

Interim Technical Report

JULY 1970

This work was supported by the U.S. Army Research Office-Durham under Grants DA-AROD-31-124-G1045 and DA-AROD-31-124-70-G51

ELECTRONIC SCIENCES LABORATORY

USC Engineering

UNCLASSIFIED

Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author)

Electronic Sciences Laboratory
University of Southern California
Los Angeles, California 90007

2a. REPORT SECURITY CLASSIFICATION

UNCLASSIFIED

2b. GROUP

3. REPORT TITLE

ON THE CROSS-CORRELATION FUNCTIONS OF MAXIMAL LINEAR RECURRING SEQUENCES

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

Scientific Interim

5. AUTHOR(S) (First name, middle initial, last name)

Herbert M. Tractenberg

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
July 1970	57	15

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
DA-AROD-31-124-G1045 ✓	USCEE 393
b. PROJECT NO.	
c.	9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)
d.	

10. DISTRIBUTION STATEMENT

This document has been approved for public release and sale; its distribution is unlimited.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	The U. S. Army Research Office-Durham, Durham, North Carolina

13. ABSTRACT

Maximal linear sequences have been studied extensively by numerous researchers. One well-known property of such sequences is their "ideal" autocorrelation property. Until recently, however, little has been known about the cross-correlation function of two different maximal sequences of the same period. Reports of research on this question which have appeared in the last few years have dealt exclusively with the case of binary sequences. In the work described herein, emphasis is on the cross-correlation of maximal linear sequences over the integers modulo p, where p is an odd prime.

DD FORM 1 NOV 65 1473

UNCLASSIFIED

Security Classification

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Maximal linear sequences						
Binary sequences						
Three-level cross-correlation						

USCEE Report 393

ON THE CROSS-CORRELATION FUNCTIONS OF MAXIMAL LINEAR RECURRING SEQUENCES

Herbert Mitchell Trachtenberg

Electronic Sciences Laboratory
University of Southern California
Los Angeles, California 90007

Interim Technical Report
A Dissertation Presented in Partial Fulfillment of Requirements
for Doctor of Philosophy (EE) Degree
JULY 1970

This work was supported by the U.S. Army Research Office-Durham
under Grants DA-AROD-31-124-G1045 and DA-AROD-31-124-70-G46

ic

ACKNOWLEDGEMENTS

The author wishes to express his gratitude to Professor S. W. Golomb, the chairman of his dissertation committee, who suggested the study of cross-correlation functions of linear recurring sequences and who advised the author throughout this work. Also acknowledged is the service of Professor A. L. Whiteman and Professor L. R. Welch on the dissertation committee. Professor Welch suggested the proof of Proposition 2 of the Appendix as well as numerous other ideas incorporated throughout the dissertation.

Along with Professors Golomb and Welch, Professors Z. A. Kaprielian, T. S. Pitcher, and W. S. Meisel served as members of the author's guidance committee and advised the author throughout his graduate work.

The author was a holder of a National Science Foundation Graduate Traineeship from 1965 to 1969 which eliminated most of the financial difficulties well-known to graduate students. The author received additional support under various government contracts with the University of Southern California Electrical Engineering Department.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER I

INTRODUCTION

I.A. Motivation

Maximal linear sequences have been studied extensively by numerous researchers. [1-7 and others] . One well-known property of such sequences is their "ideal" autocorrelation property. Until recently, however, little has been known about the cross-correlation function of two different maximal sequences of the same period. Reports of research on this question which have appeared in the last few years have dealt exclusively with the case of binary sequences [6-9] . In the work described herein, emphasis is on the cross-correlation of maximal linear sequences over the integers modulo p, where p is an odd prime.

I.B. Organization of the Dissertation

Background material on linear recurring sequences is presented in the next section. Only those aspects of the theory needed in the sequel are discussed. It is assumed that the reader has a working knowledge of modern algebra.

Chapter II is concerned with general properties of the cross-correlation function of maximal linear recurring sequences.

In Chapter III sufficient conditions for pairs of sequences to have three-level cross-correlation are given. In particular, new results are given for the case of non-binary sequences. Some mathematical propositions used in Chapter III are proved in the Appendix.

Chapter IV consists of a summary of results and some remarks.

I.C. Maximal Linear Recurring Sequences

Let $c_1, c_2, \cdots, c_n$ be elements of GF(p), p prime, with $c_n \neq 0$. A linear sequence $A = \{a_i\}$, $i = 0,1,2,\cdots$, of elements of GF(p) is a sequence which satisfies

$$a_i = c_1 a_{i-1} + c_2 a_{i-2} + \cdots + c_n a_{i-n}$$

where the arithmetic is that of GF(p). In this section some properties of ~~three~~ these sequences are given. The presentation is based on material in [1], [2], and [3] in which there is considerable overlapping of methods and results.

We first note that the n-tuple $(a_i, a_{i-1}, \cdots, a_{i-n+1})$ is completely determined by the n-tuple $(a_{i-1}, a_{i-2}, \cdots, a_{i-n})$. Since there are p^n such n-tuples which are distinct, we must have for some integer $P \leq p^n$, $(a_i, a_{i-1}, \cdots, a_{i-n-1}) = (a_{i+P}, a_{i+P-1}, \cdots, a_{i+P-n+1})$. Furthermore, since $(a_i, a_{i-1}, \cdots, a_{i-n+1}) = (0, 0, \cdots, 0)$ implies $(a_{i+1}, a_i, \cdots, a_{i-n+2}) = (0, 0, \cdots, 0)$ we see that $P \leq p^n - 1$. Hence,

Theorem 1.1: A linear sequence is periodic with period $\leq p^n-1$.

A maximal linear (recurring) sequence is a linear sequence with period exactly p^n-1. (We have yet to show that such sequences exist.)

We define the generating function associated with a linear sequence $A = \{a_i\}$ to be the power series $G(x) = \sum_{i=0}^{\infty} a_i x^i$. Since $a_i = \sum_{j=1}^{n} c_j a_{i-j}$,

$$G(x) = \sum_{i=0}^{\infty} \sum_{j=1}^{n} c_j a_{i-j} x^i$$

$$= \sum_{j=1}^{n} c_j x^j \sum_{i=0}^{\infty} a_{i-j} x^{i-j}$$

$$= \sum_{j=1}^{n} c_j x^j \left[a_{-j}x^{-j} + \cdots + a_{-1}x^{-1} + \sum_{i=0}^{\infty} a_i x^i \right]$$

$$= \sum_{j=1}^{n} c_j x^j \left[a_{-j}x^{-j} + \cdots + a_{-1}x^{-1} + G(x) \right]$$

Hence,

$$G(x) = \frac{\sum_{j=1}^{n} c_j x^j (a_{-j}x^{-j} + \cdots + a_{-1}x^{-1})}{1 - \sum_{j=1}^{n} c_j x^j}$$

We define $f(x) = 1 - \sum_{j=1}^{n} c_j x^j$ to be the characteristic polynomial associated with the sequence $a = \{a_i\}$. Note that $f(x)$ is independent of the initial conditions $(a_{-1}, a_{-2}, \cdots, a_{-n})$. The next theorems enable us to

classify the characteristic polynomials of maximal linear recurring sequences.

Theorem 1.2: If the characteristic polynomial $f(x)$ is irreducible, then the period of the linear recurring sequence $A = \{a_i\}$, $i=0, 1, \cdots$, is the smallest positive integer P for which $f(x)$ divides $x^P - 1$ modulo p, unless $a_{-1} = a_{-2} = a_{-3} = \cdots = a_{-n} = 0$, in which case A is the all zero sequence. The integer P is called the exponent of $f(x)$ because it is the smallest power of a root of $f(x)$ which equals unity.

Proof: Assume A is not the all zero sequence. The generating function $G(x) = g(x)/f(x)$. If A has period P, then

$$\sum_{i=0}^{\infty} a_i x^i = G(x)$$

$$= g(x)/f(x)$$

$$= (a_0 + a_1 x + \cdots + a_{P-1} x^{P-1})(1 + x^P + x^{2P} + \cdots)$$

$$= (a_0 + a_1 x + \cdots + a_{P-1} x^{P-1})/(1 - x^P)$$

Therefore,

$$f(x)\ (a_0 + a_1 x + \cdots + a_{P-1} x^{P-1}) = g(x)\ (1 - x^P)$$

Since $f(x)$ and $g(x)$ have no non-trivial common factors, $f(x) \mid (1 - x^P)$.

Conversely, assume $f(x) \mid (1 - x^P)$. Let the quotient be $q(x)$ of degree $< P - 1$. Since $(1 - x^P)/f(x) = q(x)$,

$$\frac{g(x)}{f(x)} = \frac{q(x)g(x)}{1 - x^P}$$

$$= g(x)q(x)(1 + x^P + x^{2P} + \cdots)$$

$$= g(x)q(x) + g(x)\, q(x)x^P + \cdots$$

$$= G(x)$$

$$= \sum_{i=0}^{\infty} a_i x^i$$

Equating coefficients of like powers of x,

$$g(x)q(x) = \sum_{i=0}^{P-1} a_i x^i$$

$$g(x)q(x)x^P = \sum_{i=0}^{P-1} a_i x^{P+i} \qquad \text{etc.,}$$

so that A has P or some factor thereof as its period. Thus, the exponent of $f(x)$ is the period of A.

Q.E.D.

Theorem 1.3: A linear recurring sequence, A, not the all zero sequence, is of maximum period, $p^n - 1$, if and only if its characteristic polynomial, $f(x)$, is primitive; i.e., if and only if the roots of $f(x)$ are primitive (p^n-1)th roots of unity.

Proof: If f(x) is primitive, it is by definition irreducible and of exponent $p^n - 1$. Therefore, by Theorem 1.2, A is of period $p^n - 1$ which, by Theorem 1.1, is maximal.

If, on the other hand, A is of maximum period, in order to show that f(x) is primitive, it will suffice to show that f(x) is irreducible, since Theorem 1.2 will then imply the exponent of f(x) is $p^n - 1$.

Assume A is of maximum period, and suppose that f(x) factors into distinct factors s(x) and t(x). Then $1/f(x) = a(x)/s(x) + b(x)/t(x)$ by the partial fraction decomposition, and s(x) and t(x) have degrees $n_1 > 0$ and $n_2 > 0$, respectively, with $n_1 + n_2 = n$. Therefore a(x)/s(x) is a power series whose coefficients are periodic with period at most $p^{n1} - 1$, and b(x)/t(x) is a power series whose coefficients have period at most $p^{n2} - 1$. Then $1/f(x) = a(x)/s(x) + b(x)/t(x)$ represents a power series whose coefficients have period at most the least common multiple of $p^{n1} - 1$ and $p^{n2} - 1$. Thus,

$$\begin{aligned} p^n - 1 &\leq (p^{n1} - 1)(p^{n2} - 1) \\ &= p^{n_1+n_2} - p^{n1} - p^{n2} + 1 \\ &\leq p^n - p - p + 1 \\ &\leq p^n - 3. \end{aligned}$$

We have a contradiction, and therefore f(x) is not a product of distinct factors.

If $f(x) = s^2(x)$, then the exponent of f(x) is at most p times that of s(x). But

$$p(p^{n/2} - 1) \leq p^n - 1.$$

In this manner we can deal with repeated factors.

Q.E.D.

Corollary: The number of translation distinct maximum length linear recurring sequences over GF(p) of period $p^n - 1$ is $\Phi(p^n - 1)/n$, where Φ is Euler's function. (For $k > 1$, $\Phi(k)$ is the number of positive integers less than k and prime to k, including 1.)

The next theorem enables us to express a maximal sequence $a = \{a_i\}$ as $a_i = T[\beta^{-i}]$ where β is a primitive $p^n - 1$ root of unity in $GF(p^n)$ and T is the trace of $GF(p^n)$ onto GF(p), i.e.

$$T(\beta) = \sum_{i=0}^{n-1} \beta^{p^i} \quad \text{for } \beta \in GF(p^n).$$

Theorem 1.4: There exists a particular phase shift of the maximal linear recurring sequence $a = \{a_i\}$ of integers modulo p, defined by the linear recurrence

$$a_i = c_1 a_{i-1} + \cdots + c_n a_{i-n} \quad i \geq 0, \; c_n \neq 0$$

with characteristic polynomial

$$f(x) = c_n x^n + \cdots + c_1 x + c_0 = -1$$

which is given by $a_1 = T\left[\lambda^{-1}\right]$, where λ is a root of $f(x)$ and is therefore, by Theorem 1.3, a primitive element of $GF(p^n)$.

Proof: We will show that the sequence $\left\{a_i\right\} = \left\{T\left[\lambda^{-i}\right]\right\}$ satisfies the linear recurrence given above.

$$\sum_{k=0}^{n} c_k a_{i-k} = \sum_{k=0}^{n} c_k T\left[\lambda^{-i+k}\right]$$

$$= \sum_{k=0}^{n} c_k \sum_{j=0}^{n-1} \lambda^{-(i-k)p^j}$$

$$= \sum_{j=0}^{n-1} \lambda^{-(i-n)p^j} \sum_{k=0}^{n} c_k \lambda^{-(n-k)p^j}$$

But $\sum_{k=0}^{n} c_k \lambda^{-(n-k)p^j}$ is identically zero for all j because λ^{-p^j} is a root of

$$f'(x) = c_0 x^n + c_1 x^{n-1} + \cdots + c_n$$

which is the reciprocal polynomial of the polynomial $f(x)$ of which λ^{p^j} is a root.

Q.E.D.

Consider the sequence $B = \left\{b_i\right\} = \left\{a_{qi}\right\}$, where $A = \left\{a_i\right\}$ is a linear recurring sequence over $GF(p)$ of period P. We say that $\left\{b_i\right\}$ is obtained by <u>decimation</u> of

$\{a_i\}$ by q. When GCD(q, P) = 1, the decimation is proper. Obviously, proper decimation cannot result in a sequence of period greater than P. Since B can be decimated by the inverse modulo P of q, which will give back A, B is a maximal sequence if and only if A is a maximal sequence.

Suppose q is a power of p modulo P. The maximal sequence $A = \{a_i\}$ satisfies the linear recurrence

$$\sum_{j=0}^{n} c_j a_{i-j} = 0, \quad i \geq 0$$

and has characteristic polynomial f(x). Then the sequence $B = \{b_i\} = \{a_{qi}\}$ satisfies the linear recurrence

$$\sum_{j=0}^{n} c_j \, b_{i-j} = \sum_{j=0}^{n} c_j \, a_{i-qj}, \quad i \geq 0.$$

Hence the characteristic polynomial of B is $f(x^q)$. But f(x) is a polynomial over GF(p). Hence, since q is a power of p, $f(x^q) = [f(x)]^q$, and $f(x^q) = 0$ if and only if $f(x) = 0$. Since their characteristic polynomials have the same roots, A and B are the same sequences except for a phase shift. We therefore have

Theorem 1.5: Let $A = \{a_i\}$ be a maximal linear recurring sequence of period $p^n - 1$. The sequence $B = \{b_i\} = \{a_{qi}\}$ is also a maximal linear recurring sequence if and only if q and $p^n - 1$ are relatively prime. Furthermore, when q is a power of p modulo $p^n - 1$, A and B are the same sequence except for a phase shift.

Theorem 1.6: Let $\{a_i\}$ be a maximal linear recurring sequence of period $p^n - 1$, and let $\{b_i\}$ be another such sequence. Then $\{b_i\}$ can be obtained from $\{a_i\}$ by proper decimation. (This is the converse of Theorem 1.5)

Proof: By Theorem 1.4, $a_i = T[\lambda^{-i}]$, $i = 0,1,2, \cdots$, where λ is primitive in $GF(p^n)$. Also, $b_i = T[\zeta^{-i}]$, $i = 0,1,2,\cdots$, where ζ is primitive in $GF(p^n)$. But $\zeta = \lambda^q$ for some q such that $GCD(q, p^n - 1) = 1$. Hence, $b_i = T[\zeta^{-i}] = T[\lambda^{-qi}] = a_{qi}$.

Q.E.D.

Consider, now, the factorization of $x^{p^n} - x$ into irreducible factors over GF(p). Let ω be an element of $GF(p^n)$, $\omega \neq 0$. Then the distinct elements of the set $\{\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{n-1}}\}$ are the roots of one irreducible factor of $x^{p^n} - x$. The set $H = \{1, p, p^2, \cdots, p^{n-1}\}$ is a subgroup of the multiplicitive group of the integers modulo $p^n - 1$. For integer q, the set $qH = \{q, qp, qp^2, \cdots, qp^{n-1}\}$ is called a cyclotomic coset. When $GCD(q, p^n - 1) = 1$, qH is called a proper cyclotomic coset. For λ a primitive $p^n - 1$ root of unity, the distinct elements of the set $\{\lambda^q, \lambda^{qp}, \cdots, \lambda^{qp^{n-1}}\}$ are the roots of one irreducible factor of $x^{p^n} - x$. If qH is a proper cyclotomic coset, the associated factor is primitive of degree n. Otherwise, the associated factor is not primitive and is of degree $m \leq n$, where m is the

number of distinct elements in the cyclotomic coset.

We saw in Theorem 1.4 that we can express any maximal linear recurring sequence $A = \{a_i\}$ in terms of the trace of $GF(p^n)$ onto $GF(p)$. For integer m, and $\beta \in Gf(p^n)$, so that $\beta^{p^n} = \beta$, $T[\beta^{p^m}] = T[\beta]$. Hence for λ primitive in $GF(p^n)$, $a_i = T[\lambda^{-i}]$ depends only on the cyclotomic coset to which i belongs and not on the specific value of i. When this is the case, the sequence is said to be in a natural orientation. When A is a maximal sequence in natural orientation, it is clear that $A = \{a_i\}$, $2A = \{2a_i\}$, $\cdots$, $(p-1)A = \{(p-1)a_i\}$ are all phase shifts of A and are all in natural orientation. Furthermore, since $a_{ip^m} = T[\lambda^{-ip^m}] = T[\lambda^{-i}] = a_i$, decimating a maximal sequence in natural orientation by a power of p (modulo the period of the sequence) results in the same sequence in the same phase.

CHAPTER II

CORRELATION PROPERTIES OF MAXIMAL LINEAR RECURRING SEQUENCES

II.A. Autocorrelation

Let $A = \{a_i\}$ be a maximal linear recurring sequence over GF(p) of length $p^n - 1$. We define the (unnormalized) autocorrelation function of A to be

$$C(\tau) = \sum_{i=0}^{p^n-2} \chi(a_i)\chi^*(a_{i+\tau})$$

where $\chi(a) = \rho^a$, ρ a primitive p^{th} root of unity, and where $\chi^*(a) = \chi(-a)$ is the complex conjugate of $\chi(a)$.

Theorem 2.1: [1,2,3]

$$C(\tau) = \begin{cases} -1 & , \quad \tau \not\equiv 0 \bmod p^n-1 \\ p^n-1 & , \quad \tau \equiv 0 \bmod p^n-1 \end{cases}$$

Proof: Suppose $\tau \equiv 0 \bmod p^n-1$, so that $a_i = a_{i+\tau}$. Then $\chi(a_i)\ \chi^*(a_{i+\tau}) = \chi(a_i)\ \chi^*(a_i) = \rho^{a_i - a_i} = 1$.

Therefore, $C(\tau) = \sum_{i=0}^{p^n-2} \chi(a_i)\ \chi^*(a_{i+\tau}) = p^n-1$.

Suppose $\tau \not\equiv 0 \bmod p^n-1$. Then $\chi(a_i)\ \chi^*(a_{i+\tau}) = \rho^{a_i}\rho^{-a_i+\tau} = \rho^{a_i - a_i+\tau}$. But $\{a_i\}$ satisfies a linear recurrence $\sum_{j=1}^{n} c_j a_{i-j} = 0$, $c_0 = -1$, and $\{b_i\} = \{a_{i+\tau}\}$

satisfies the same linear recurrence, $\sum_{j=1}^{n} c_j b_{i-j} = 0$, $c_o = -1$. Therefore, $\sum_{j=1}^{n} c_j(a_{i-j}-b_{i-j}) = \sum_{j=1}^{n} c_j(a_{i-j}-a_{i+\tau-j}) = 0$ and $\{a_i - a_{i+\tau}\}$ satisfies the same linear recurrence and is therefore a phase shift of $\{a_i\}$. In one period of a maximal linear recurring sequence of period p^n-1, each element of GF(p) except the zero element appears p^n-1 times. The zero element appears p^n-1 times. Thus

$$C(\tau) = \sum_{j=1}^{p^n-2} \rho^{a_i-a_{i+\tau}} = (p^{n-1}-1)\rho^0 + \sum_{k=1}^{p-1} p^{n-1}\rho^k .$$

But the powers of a primitive p^{th} root of unity sum to zero. Thus, $C(\tau) = -1$.

Q.E.D.

II.B. Cross-Correlation

Let $A = \{a_i\}$ be a maximal linear recurring sequence over GF(p) of period p^n-1. Let $B = \{b_i\}$ be another such sequence. We saw in Chapter I that B can be written $\{b_i\} = \{a_{qi}\}$ with q relatively prime to p^n-1, and that A and B are distinct when q is not a power of p modulo p^n-1. We define the (unnormalized) cross-correlation function of A and B to be

$$C_{AB}(\tau) = C_q(\tau) = \sum_{i=0}^{p^n-2} \chi(a^i)\chi^*(a_{qi+\tau})$$

where $\chi(a) = \rho^a$, ρ a primitive p^{th} root of unity, and $\chi^*(a) = \chi(-a)$ is the complex conjugate of $\chi(a)$.

Theorem 2.2: The set of values assumed by $C_q(\tau)$, the cross-correlation of maximal linear recurring sequences $\{a_i\}$ and $\{b_i\}$ of period p^n-1, is independent of which primitive p^{th} root of unity, ρ, is used in the definition of $C_q(\tau)$. (It is not in general true that the value of $C_q(\tau)$ for a specific value of τ is independent of which primitive root of unity is chosen.)

Proof: Consider $C_q(\tau)$ defined using the primitive p^{th} root of unity ρ.

$$C_q(\tau) = \sum_{i=0}^{p^n-2} \rho^{a_i - b_{i+\tau}}$$

Suppose ρ is replaced by ρ^m, $1 < m < p$.

$$\sum_{i=0}^{p^n-2} (\rho^m)^{a_i - b_{i+\tau}} = \sum_{i=0}^{p^n-2} \rho^{(ma_i - mb_{i+\tau})}$$

But because $\{a_i\}$ and $\{b_i\}$ are maximal sequences, $\{ma_i\}$ is a phase shift of $\{a_i\}$ and $\{mb_{i+\tau}\}$ is a phase shift of $\{b_{i+\tau}\}$. Hence,

$$\sum_{i=0}^{p^n-2} (\rho^m)^{a_i - b_{i+\tau}} = \sum_{i=0}^{p^n-2} \rho^{a_{i+\sigma} - b_{i+\tau+\mu}}$$

$$= C_q(\tau)$$

for $\tau' = \tau + \mu - \sigma$.

Q.E.D.

Theorem 2.3: The cross-correlation function, $C_q(\tau)$, of two maximal linear sequences of length $p^n - 1$ over GF(p) is real for all τ.

Proof: For $p = 2$, $\rho = -1$. Let $p > 2$. Then $p^n - 1$ is even. Since the sequences are linear, the second half of a period of a sequence, relative to any starting point, is the negative of the first half. Let the sequences by $\{a_i\}$ and $\{b_i\}$. Then

$$C_{AB}(\tau) = \sum_{i=1}^{p^n-1} \chi(a_i)\, \chi^*(b_{i+\tau})$$

$$= \sum_{i=1}^{(p^n-1)/2} \chi(a_i - b_{i+\tau}) + \sum_{i=(p^n+1)}^{p^n-1} \chi(a_i - b_{i+\tau})$$

$$= \sum_{i=1}^{(p^n-1)/2} \left[\chi(a_i - b_{i+\tau}) + \chi(-a_i + b_{i+\tau})\right]$$

$$= \sum_{i=1}^{(p^n-1)/2} \left[\chi(a_i - b_{i+\tau}) + \chi^*(a_i - b_{i+\tau})\right]$$

$$= 2\,\mathrm{Re} \sum_{i=1}^{(p^n-1)/2} \chi(a_i - b_{i+\tau})$$

Q.E.D.

Theorem 2.4: The cross-correlation function, $C_q(\tau)$, depends on the cyclotomic coset to which q belongs and not on the specific value of q. [1,2,3]

Proof: The cross-correlation is

$$C_q(\tau) = \sum_{i=1}^{p^n-1} \chi(a_i - \tau)\, \chi^*(a_{qi}).$$

But by Theorem 1.5, a_{qi} and $a_{q'i}$ are equal for all i when q' is in the same cyclotomic coset as q.

Q.E.D.

Theorem 2.5: Let $\{a_i\}$ be a maximal linear recurring sequence of period p^n-1. Let q be prime to the period of $\{a_i\}$ and let q' be such that $qq' \equiv 1$ modulo p^n-1. Then the cross-correlation of $\{a_i\}$ and $\{a_{qi}\}$, $C_q(\tau)$, assumes the same values as the cross-correlation of $\{a_i\}$ and $\{a_{q'i}\}$, $C_{q'}(\sigma)$, although not generally in the same order. In particular, $C_q(\tau) = C_{q'}(-q'\tau)$.

Proof: By definition, for ρ a primitive p^{th} root of unity,

$$C_q(\tau) = \sum_{j=0}^{p^n-2} \rho^{a_j - a_{qj} + \tau}$$

$$= \sum_{j=0}^{p^n-2} \rho^{a_j - a_q(j+q'\tau)}$$

Similarly,

$$C_{q'}(\sigma) = \sum_{j=0}^{p^n-2} \rho^{a_j - a_{q'j} + \sigma}$$

$$= \sum_{j=0}^{p^n-2} \rho^{a_j - \sigma - a_{q'j}}$$

$$= \sum_{j=0}^{p^n-2} \rho^{a_q(j-\sigma) - a_j}$$

$$= \sum_{j=0}^{p^n-2} (\alpha^{-1})^{a_j - a_q(j-\sigma)}$$

But replacing α by α^{-1} or vice versa in the expression for cross-correlation gives us the complex conjugate of the correlation value. However, by Theorem 2.3, the cross-correlation is real valued. Hence replacing α by α^{-1} does not change the cross-correlation value. Therefore,

$$C_q(\tau) = C_{q'}(-q'\tau).$$

Q.E.D.

CHAPTER III

MAXIMAL LINEAR RECURRING SEQUENCES WITH THREE-LEVEL CROSS-CORRELATION

III.A. Introduction

We consider here the cross-correlation of maximal linear recurring sequences over GF(p) of period p^n-1. We saw in Chapter I that if such a sequence $A = \{a_i\}$ is in one of its p-1 "natural orientations," then $B = \{b_i\} = \{a_{qi}\}$ is also a maximal linear recurring sequence in a "natural orientation" whenever q and p^n-1 are relatively prime. We saw also that sequences A and B are distinct when q is not a power of p.

As before, we define

$$C_{AB}(\tau) = C_q(\tau) = \sum_{i=0}^{p^n-2} \chi(a_{i-\tau})\, \chi^*(a_{qi})$$

where $\chi(a) = \rho^a$, and ρ is a primitive p^{th} root of unity. In this chapter we ask for which values of q, $C_q(\tau)$ takes on exactly three distinct values. In the next section various conditions sufficient for this to occur in the case p=2 are summarized. In subsequent sections the case of p an odd prime is considered in detail.

III.B. Sufficient Conditions for Three-Valued Cross-Correlation in the Case p = 2

Here we consider maximal linear recurring binary

sequences of length 2^n-1, and ask for which q, $C_q(\tau)$ assumes exactly three values.

Theorem 3.1: Any $q = 2^k + 1$ such that $\frac{n}{GCD(k,n)}$ is odd leads to three-valued cross-correlation. The values which occur are -1 and $-1 \pm 2^{(n+e)/2}$ where $e = GCD(k,n)$. [5] [6] [8] [9]

Theorem 3.2: If $\frac{n}{GCD(k,n)}$ is odd, then $q = 4^k-2^k+1$ leads to three-valued cross-correlation where the values which occur are again -1 and $-1 \pm 2^{(n+e)/2}$, where $e = GCD(n,k)$. [7]

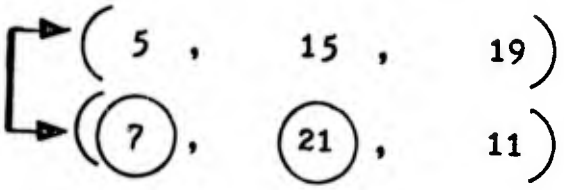
It is further conjectured (by L. Welch) that the specific choice of $a = 2^{(n-1)/2} + 3$ leads to three-level cross-correlation for all odd n. This has been verified by computation for odd $n \leq 15$.

III.C. Data for the Case of p an Odd Prime

The cross-correlation function $C_q(\tau)$ of all distinct pairs of maximal linear recurring sequences of length p^n-1 were computed for various p and n. The tables in this section list the values of q for which three-level cross-correlation was observed. Since for any q which leads to three-level cross-correlation, all other members of its cyclotomic coset do likewise, the data is arranged

in cyclotomic cosets. As was seen in Chapter II, values of q in a particular cyclotomic coset leading to three-level cross-correlation implies values in the inverse cyclotomic coset--that is, the coset containing q' such that $qq' \equiv 1 \bmod (p^n-1)$--also leads to three-level cross-correlation. For this reason, inverse pairs of cosets are indicated by arrows.

The values of q predicted by Theorem 3.3, which is proved in the next section, are enclosed in a square. The values of q predicted by Theorem 3.4 are enclosed in a circle. These values, together with the values of q in the same and the inverse cyclotomic cosets account for most occurrences of three-level cross-correlation. Asterisks to the right of the cosets indicate those consisting of values which are not predicted by any known theorem.



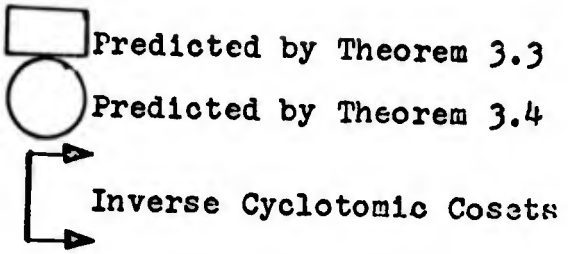


Table 3.1. Values of q Resulting in Three-Level $C_q(\tau)$, p = 3, n = 3

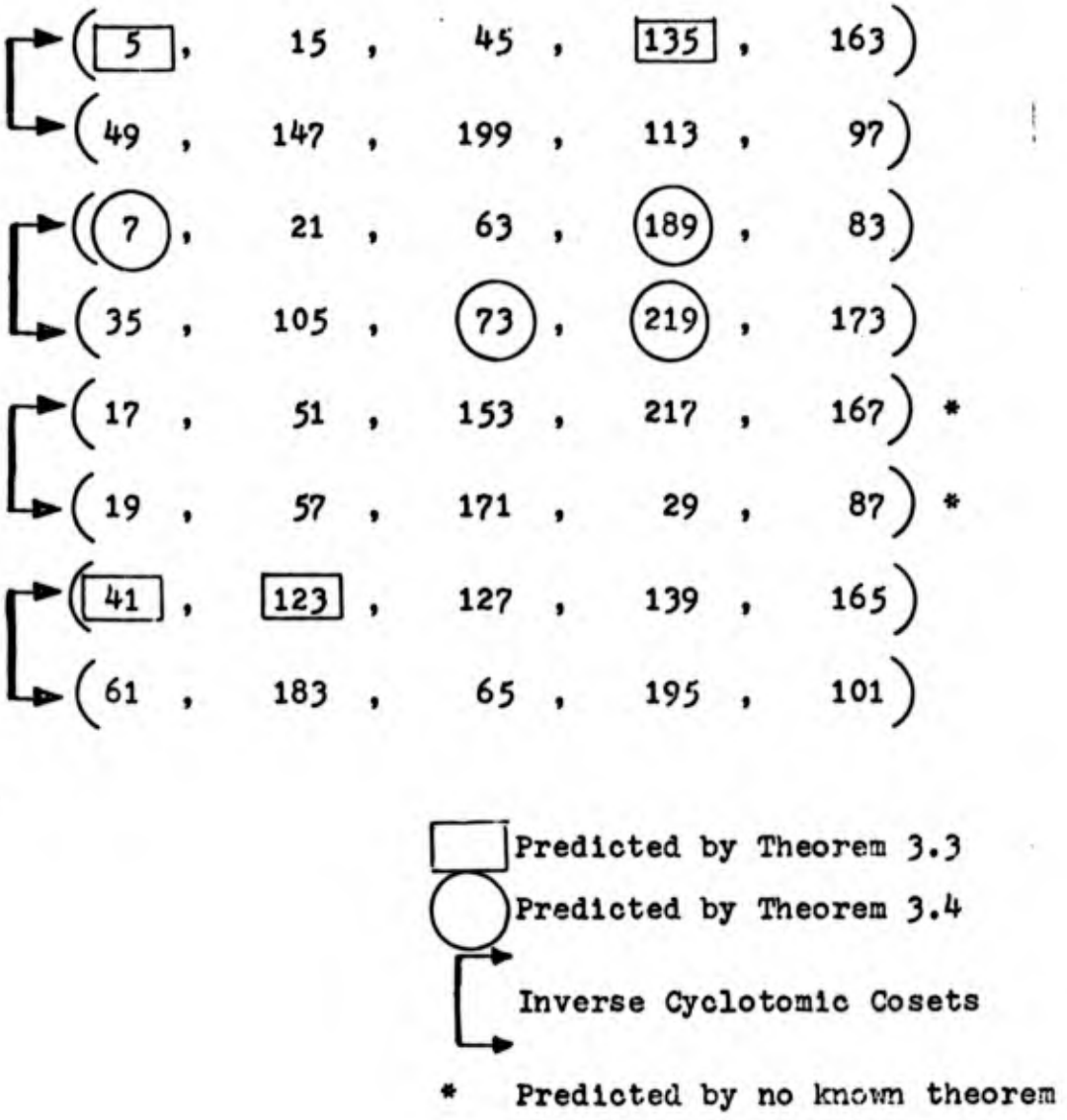
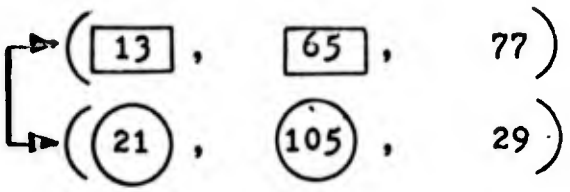


Table 3.2. Values of q Resulting in Three-Level $C_q(\tau)$, p = 3, n = 5

(5	15	45	135	405	1215	1459)	
(439	1317	1765	923	583	1749	875)	
(7	21	63	189	567	1701	731)	
(347	1041	937	625	1875	1253	1573)	
(11	33	99	297	891	487	1461)	*
(199	597	1791	1001	817	265	795)	*
(41	123	369	1107	1135	1219	1471)	
(391	1173	1333	1813	1067	1015	859)	
(53	159	477	1431	2107	1949	1475)	*
(55	165	495	1485	83	249	747)	*
(61	183	549	1647	569	1707	749)	
(73	219	657	1971	1541	251	753)	
(107	321	963	703	2109	1955	1473)	
(227	681	2043	1757	899	511	1533)	
(365	1095	1099	1111	1147	1255	1579)	
(547	1641	551	1653	587	1761	911)	

Table 3.3. Values of q Resulting in Three-Level $C_q(\tau)$, $p = 3$, $n = 7$.

See Legend, Table 3.2.



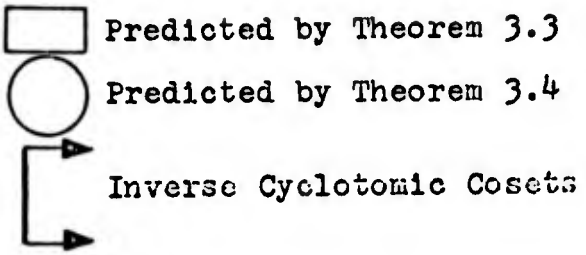


Table 3.4. Values of q Resulting in Three-Level $C_q(\tau)$, p = 5, n = 3

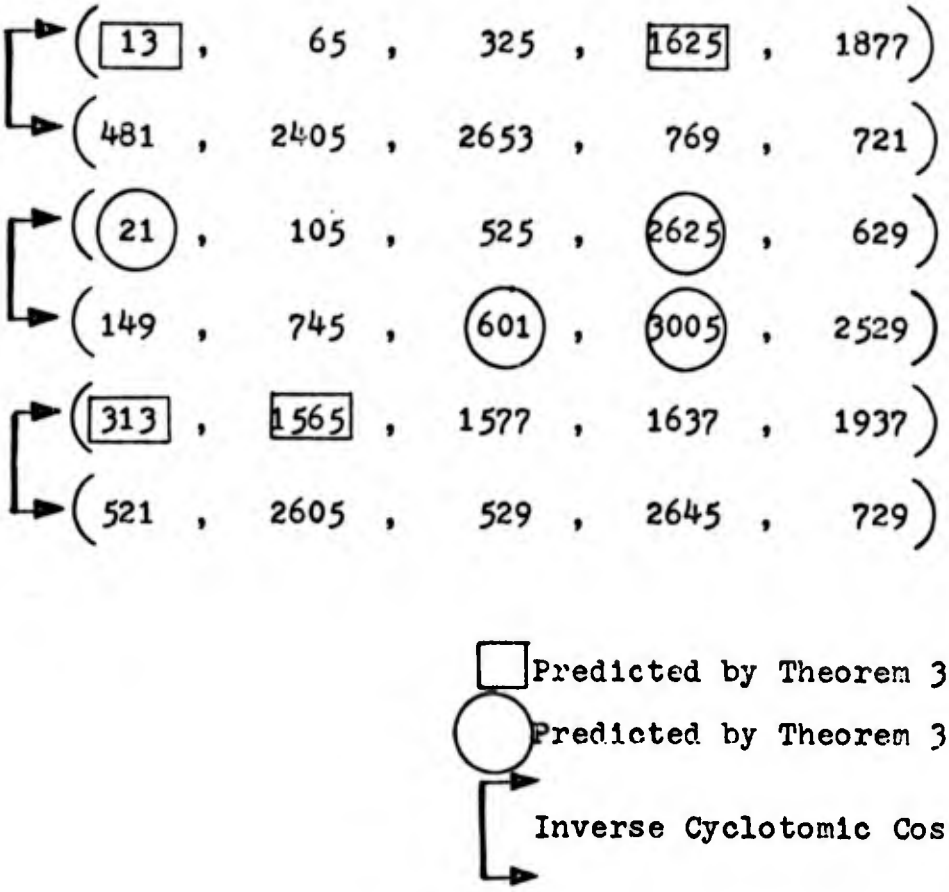
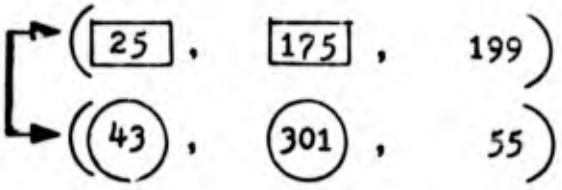


Table 3.5. Values of q Resulting in Three-Level $C_q(\tau)$, p = 5, n = 5



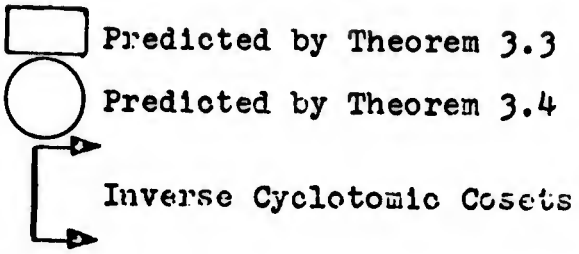


Table 3.6. Values of q Resulting in Three-Level $C_q(\tau)$, p = 7, n = 3

III.D. Sufficient Conditions for Three-Valued Cross-Correlation in the Case of p an Odd Prime

In this section two new theorems are proved.

Theorem 3.3: Let $\{a_i\}$ be a maximal linear recurring sequence over GF(p) of length p^n-1, with p an odd prime and with n odd. Let $\{b_i\}$ be the sequence $\{a_{qi}\}$ with $q = (p^{2k} + 1)/2$ not congruent to a power of p modulo $(p^n - 1)$. Let ρ be a primitive p^{th} root of unity. Then $\{b_i\}$ is also a maximal linear recurring sequence, and the cross-correlation of $\{a_i\}$ and $\{b_i\}$ defined by

$$C_q(\tau) = \sum_{i=0}^{p^n-2} \chi(a_i)\, \chi^*(a_{qi})$$

where $\chi(a) = \rho^a$, assumes one of three values, -1 or $-1 \pm p^{(n+e)/2}$ where $e = GCD(k,n)$.

Theorem 3.4: With the same premises as Theorem 3.3, except $q = p^{2k}-p^k+1$, $\{b_i\}$ is a maximal linear recurring sequence and the cross-correlation of $\{a_i\}$ and $\{b_i\}$, $C_q(\tau)$, again assumes one of the three values, -1 or $-1 \pm p^{(n+e)/2}$ where $e = GCD(k,n)$.

In order to prove Theorems 3.3 and 3.4, we require several lemmas.

Lemma 3.1: For p an odd prime and n odd, $GCD(p^k + 1,\ p^n - 1) = 2$.

Proof: Suppose an odd prime q divides GCD(p^k+1, p^n-1). Let e be the exponent of p modulo q. Pick a and r, $0 \leq r < e$, such that $k = ae+r$. Then $p^k = p^{ae} \cdot p^r = (p^e)^a \cdot p^r = p^r \equiv -1 \pmod q$. Hence, $p^{2r} \equiv 1 \pmod q$. But $0 < 2r < 2e$ implies $2r = e$ and e is therefore even. But e divides n since $p^n \equiv 1 \pmod q$. Hence 2 divides n, which is a contradiction. It remains to be shown that GCD(p^k+1, p^n-1) is not divisible by 4. Suppose $p \equiv 1 \pmod 4$. Then 4 divides p^n-1 for all n, but 4 does not divide p^k+1 for any k. If $p \equiv -1 \pmod 4$, then odd n implies $p^n-1 \equiv -2 \pmod 4$.

Q.E.D.

Lemma 3.2: For p an odd prime and n odd, GCD $\left(\frac{p^{2k}+1}{2}, p^n-1\right) = 1$.

Proof: Assume 4 divides $p^{2k}+1$. Then $p^{2k} \equiv -1 \pmod 4$ and $p^k \equiv \sqrt{-1} \pmod 4$. But -1 is a not-square modulo 4, hence 4 does not divide $p^{2k}+1$. By Lemma 3.1, GCD($p^{2k}+1$, p^n-1) = 2.

Q.E.D.

Lemma 3.3: For p an odd prime and n odd, GCD($p^{2k}-p^k+1$, p^n-1) = 1.

Proof: By Lemma 3.1, GCD($p^{3k}+1$, p^n-1) = 2. Since

$p^{2k}-p^k+1 = (p^{3k}+1)/p^k+1$ is odd, the assertion follows.

Q.E.D.

Lemma 3.4: (cf. [10, § 62]) The not-squares of GF(p), $p > 2$, are not-squares in $GF(p^n)$ if and only if n is odd.

Proof: Let λ be a primitive element of $GF(p^n)$. Then $\rho = \lambda^u$, where $u = (p^n-1)/(p-1)$, is a primitive element of GF(p). Let ρ^v be a not-square in GF(p), so that v is odd. Then $\rho^v = \lambda^{uv}$ will be a not-square in $GF(p^n)$ if and only if uv is odd, i.e., if and only if u is odd. But $u = \sum_{i=0}^{n-1} p^i$ = sum of n odd terms. Hence, u is odd if and only if n is odd.

Q.E.D.

Lemma 3.5: The number of sets of solutions $(a_1, a_2, \cdots, a_{2m})$ in GF(p), $p > 2$, of the quadratic equation

$$c_1a_1^2 + c_2a_2^2 + \cdots + c_{2m}a_{2m}^2 = c$$

where every c_i is a nonzero element of GF(p) and $c \in GF(p)$ is

$$p^{2m-1}-up^{m-1} \qquad (c \neq 0)$$

$$p^{2m-1} + u\left[p^m-p^{m-1}\right] \qquad (c = 0)$$

where u is +1 or -1 according to whether $(-1)^m c_1c_2\cdots c_{2m}$

is a square or a not-square in GF(p). [10, § 65]

Lemma 3.6: The number of sets of solutions in GF(p), $p > 2$, of the quadratic equation

$$c_1 a_1^2 + c_2 a_2^2 + \cdots + c_{2m+1} a_{2m+1}^2 = c$$

where every c_i is a nonzero element of GF(p) and $c \in GF(p)$ is $p^{2m} + up^m$, where u is +1, -1, or 0, as $(-1)^m c\, c_1 c_2 \cdots c_{2m+1}$ is a square, a not-square, or zero in the field, respectively. [10, § 66]

Proof of Theorem 3.3: By Lemma 3.2, $\mathrm{GCD}\left(\frac{p^{2k}+1}{2}, p^n-1\right) = 1$. Thus $\{b_i\} = \{a_{qi}\}$ is a maximal linear recurring sequence which, since q is not a power of p modulo (p^n-1), is distinct from the sequence $\{a_i\}$.

Let λ be a primitive element in $GF(p^n)$. By Theorem 1.4, we can write $a_i = T(\lambda^{-i})$ where T is the trace of $GF(p^n)$ onto GF(p). Hence,

$$\begin{aligned} C_q(\tau) &= \sum_{i=0}^{p^n-2} \chi\left(T\left[\lambda^{-(i-\tau)}\right]\right) \chi^*\left(T\left[\lambda^{-iq}\right]\right) \\ &= \sum_{i=0}^{p^n-2} \chi\left(T\left[\lambda^{-(i-\tau)}\right] - T\left[\lambda^{-i(p^{2k}+1)/2}\right]\right) \\ &= \sum_{i=0}^{p^n-2} \chi\left(T\left[\lambda^{-(i-\tau)} - \lambda^{-i(p^{2k}+1)/2}\right]\right) \\ &= \left\{ \sum_{x \in GF(p^n)} \chi\left(T\left[\gamma x - x^{(p^{2k}+1)/2}\right]\right) \right\} - 1 \end{aligned}$$

where $\gamma = \lambda^{\tau}$ and we have used the fact that $T(0) = 0$. We can evaluate this expression if we can determine for how many $x \in GF(p^n)$, $T\left[\gamma x - x^{(p^{2k}+1)/2}\right]$ assumes the value of each element of $GF(p^n)$.

Let $x = y^2$. As y becomes each nonzero element of $GF(p^n)$, x becomes each even power of λ twice; and x is the zero element when y is the zero element. Similarly, consider $x = dy^2$ where d is a not-square of GF(p) and hence is, by Lemma 3.4, a not-square of $GF(p^n)$. Therefore, d is an odd power of λ ; and as y becomes each nonzero element of $GF(p^n)$, x becomes each odd power of λ twice and is the zero element when y is the zero element.

Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be a basis in $GF(p^n)$. Then $y \in GF(p^n)$ can be written $y = \sum_{i=1}^{n} a_i \alpha_i$ where $a_i \in GF(p)$, $i=1, \cdots, n$; and

$$y^2 = \sum_{i=1}^{n} a_i \alpha_i \sum_{j=1}^{n} a_j \alpha_j$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{n} a_i a_j \alpha_i \alpha_j$$

Similarly,

$$y^{p^{2k}+1} = \sum_{i=1}^{n} a_i^{p^{2k}} \alpha_i^{p^{2k}} \sum_{j=1}^{n} a_j \alpha_j$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{n} a_i a_j \alpha_i^{p^{2k}} \alpha_j$$

where we have made use of the fact that for a and b elements of a field of characteristic p,

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}$$

and for a in GF(p), $a^p = a$.

For $\underline{x} = y^2$ we therefore have

$$T\left[\gamma\, x - x\,\frac{p^{2k}+1}{2}\right]$$

$$= T\left[\gamma\, y^2 - y^{p^{2k}+1}\right]$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{n} a_i a_j\, T\left[\gamma\,\alpha_i\alpha_k - \alpha_1^{p^{2k}}\,\alpha_j\right]$$

where we have made use of the linearity of the trace function over GF(p).

Now, since $d \in GF(p)$, and since p is prime,

$$d^{p^k} \equiv d \pmod{p}$$

which implies

$$d^{p^k-1} \equiv 1 \pmod{p}$$

which implies

$$\left[d^{p^k-1}\right]^{\frac{p^k+1}{2}} \equiv 1 \pmod{p}$$

which implies

$$d^{\frac{p^{2k}-1}{2}} \equiv 1 \pmod{p}$$

which implies

$$d^{\frac{p^{2k}+1}{2}} \equiv d \pmod{p}.$$

Thus for $x = dy^2$ we have

$$T\left[\gamma x - x^{\frac{p^{2k+1}}{2}}\right]$$

$$= T\left[\gamma\, dy^2 - d^{\frac{p^{2k+1}}{2}}\, y^{p^{2k+1}}\right]$$

$$= d\sum_{i=1}^{n}\sum_{j=1}^{n} a_i a_j\, T\left[\gamma\, \alpha_i\alpha_j - \alpha_i^{p^{2k}}\alpha_j\right]$$

Setting $b_{ij} = b_{ji}$

$$= \frac{1}{2}\left(T\left[\gamma\, \alpha_i\alpha_j - \alpha_i^{p^{2k}}\alpha_j\right]\right.$$

$$\left. + T\left[\gamma\, \alpha_j\alpha_i - \alpha_j^{p^{2k}}\alpha_i\right]\right)$$

which is an element of GF(p), we have two quadratic forms, identical except for the constant factor d which is a not-square in GF(p):

$$f(y) = T\left[\gamma\, y^2 - y^{2\left(\frac{p^{2k+1}}{2}\right)}\right]$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij} a_i a_j$$

and

$$T\left[\gamma\, dy^2 - (dy^2)^{\frac{p^{2k+1}}{2}}\right]$$

$$= d\sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij} a_i a_j$$

$$= d\, f(y).$$

We can now write f(y) in canonical form. [11, §113] That is, there exists a linear transformation of $(a_1, \cdots, a_n)$ and there exist $c_i \in GF(p)$, $c_i \neq 0$, $i = 1, \cdots, s$ and $s \leq n$ such that

$$f(y) = \sum_{i=1}^{s} c_i a_i^2$$

Recall that we are trying to determine for how many $x \in GF(p^n)$ the equation

$$T\left[\gamma x - x^{(p^{2k}+1)/2}\right] = c$$

is satisfied for each c in GF(p). We can do this by determining for how many $y \in GF(p^n)$, f(y) and d f(y) assume the value c, and then dividing the total by two. We divide by two because by studying f(y) and d f(y) for each y in $GF(p^n)$ we will have considered $T\left[\gamma x - x^{(p^{2k}+1)/2}\right]$ twice for each x in $GF(p^n)$.

We can apply Lemmas 3.5 and 3.6 if we can determine s--that is, if we can determine the rank of the quadratic form f(y). But f(y) is independent of n-s coordinates. To find n-s, we must determine the number of z's in $GF(p^n)$ such that f(y+z) = f(y) for all y in $GF(p^n)$.

$$0 = f(y+z) - f(y)$$

$$= T\left[\gamma (y+z)^2 - (y+z)^{p^{2k}+1}\right] - T\left[\gamma y^2 - y^{p^{2k}+1}\right]$$

$$= T\left[\gamma (y^2 + 2yz + z^2) - (y^{p^{2k}} + z^{p^{2k}})(y+z) - \gamma y^2 + y^{p^{2k}+1}\right]$$

$$= T\left[2\gamma yz + \gamma z^2 - yz^{p^{2k}} - y^{p^{2k}} z - z^{p^{2k}+1}\right]$$

$$= T\left[\gamma z^2 - z^{p^{2k}+1} + y^{p^{2k}} \left(z^{p^{2k}} (2\gamma)^{p^{2k}} - z^{p^{4k}} - z\right)\right]$$

If the above equation is to hold for all y in $GF(p^n)$, z must satisfy

$$z^{p^{4k}} - (2\gamma)^{p^{2k}} z^{p^{2k}} + z = 0$$

By Proposition 1 of the Appendix, there are exactly $1 = p^o$, p^e, or p^{2e} such z's in $GF(p^n)$ where $e = GCD(k,n)$. Hence, s equals n, n-e, or n-2e.

Assume first that s = n-e which is even. Note that $(-1)^{\frac{s}{2}}(dc_1)(dc_2)\cdots(dc_s)$ and $(-1)^{\frac{s}{2}}c_1c_2\cdots c_s$ are both squares or are both not-squares in GF(p). Assume both are squares. Then, by Lemma 3.5 the number of solutions in $GF(p^n)$ to <u>each</u> of the equations f(y) = c and d f(y) = c is

$$p^{s-1} - p^{\frac{s}{2}-1} \quad , c \neq 0$$

$$p^{s-1} + p^{\frac{s}{2}} - p^{\frac{s}{2}-1} \quad , c = 0.$$

However, since we are really interested in the number of roots in $GF(p^n)$ of

$$T\left[\gamma x - x^{p^{\frac{2k+1}{2}}} = c\right]$$

we multiply the above numbers by p^{n-s} to account for all x in $GF(p^n)$. Thus for s even and $(-1)^{s/2}c_1c_2\cdots c_s$ a square in GF(p), the number of roots in $GF(p^n)$ is

$$p^{n-1} - p^{n-\frac{s}{2}} - 1 \quad , c \neq 0$$

$$p^{n-1} + p^{n-\frac{s}{2}} - p^{n-\frac{s}{2}} - 1 \quad , c = 0$$

Since the primitive p^{th} roots of unity sum to -1, and since in this case s = n-GCD(k,n), we have

$$C_q(\tau) = -1 + \sum_{x \in GF(p^n)} \omega^{T\left[\gamma x - x^{(p^{2k}+1)/2}\right]}$$

$$= -1 + p^{\frac{n+e}{2}}$$

where e = GCD(k,n).

Similarly, for $(-1)^{s/2} c_1 c_2 \cdots c_s$ a not-square in GF(p)

$$C(\tau) = -1 - p^{\frac{n+e}{2}} .$$

We still must consider the cases when n-s = o and when n-s = 2e. In both cases s is odd, and we can apply Lemma 3.6. Note that if $(-1)^{(s-1)/2}\, c\, c_1 \cdots c_s$ is a square, then $(-1)^{(s-1)/2} c (dc_1)(dc_2) \cdots (dc_s)$ is a not-square in GF(p), and conversely. Hence, in this case $T\left[\gamma x - x^{(p^{2k}+1)/2}\right]$ assumes each value of GF(p) an equal number of times and we have

$$C(\tau) = -1.$$

Q.E.D.

Proof of Theorem 3.4: By Lemma 3.3, $GCD(p^{2k}-p^k+1, p^n-1) = 1$. Thus $\{b_i\} = \{a_{qi}\}$ is a maximal linear recurring sequence which, since q is not a power of p modulo (p^n-1), is distinct from the sequence $\{a_i\}$.

We proceed as in the proof of Theorem 3.3. Let be a primitive element in $GF(p^n)$. By Theorem 1.4, we can write $a_i = T(\lambda^{-i})$ where T is the trace of $GF(p^n)$ onto $GF(p)$. Hence,

$$C_q(\tau) = \sum_{i=0}^{p^n-2} \chi\left(T\left[\lambda^{-(i-\tau)}\right]\right) \chi^*\left(T\left[\lambda^{-iq}\right]\right)$$

$$= \sum_{i=0}^{p^n-2} \chi\left(T\left[\lambda^{-(i-\tau)}\right] - T\left[\lambda^{-i(p^{2k}-p^k+1)}\right]\right)$$

$$= \sum_{i=0}^{p^n-2} \chi\left(T\left[\lambda^{-(i-\tau)} - \lambda^{-i(p^{2k}-p^k+1)}\right]\right)$$

$$= \left\{ \sum_{x \in GF(p^n)} \chi\left(T\left[\gamma x - x^{p^{2k}-p^k-1}\right]\right)\right\} - 1$$

where $\gamma = \lambda^{\tau}$ and we have used the fact that $T(0) = 0$. We can evaluate this expression if we can determine for how many $x \in GF(p^n)$, $T\left[\gamma x - x^{p^{2k}+1}\right]$ equals each element of $GF(p)$.

Let $x = y^{p^k+1}$. By Lemma 3.1, $GCD(p^k+1, p^n-1) = 2$. Therefore, as y becomes each nonzero element of $GF(p^n)$, x becomes each even power of λ twice. When y is the zero element, x is the zero element. Similarly, consider $x = dy^{p^k+1}$ where d is a not-square of GF(p) and hence is, by Lemma 3.4, a not-square of $GF(p^n)$. Therefore, d is an odd power of λ ; and as y becomes each nonzero element of $GF(p^n)$, x becomes each odd power of λ twice and is the zero element when y is the zero element.

Making use of the fact that $d \in GF(p)$ so that $d^{p^{2k}} - p^k + 1 = d$ we proceed exactly as in the proof of Theorem 3.3 to get two quadratic forms,

$$f(y) = T\left[\gamma\, y^{p^k+1} - y(p^k+1)(p^{2k}-p^k+1)\right]$$

and

$$df(y) = T\left[\gamma\, dy^{p^k+1} - dy^{p^k+1}\, p^{2k}-p^k+1\right]$$

which are identical except for the constant factor d which is an element of GF(p).

We can apply Lemmas 3.5 and 3.6 if we can determine the rank of f(y). But f(y) is independent of n-s coordinates. To find n-s, we must determine the number of z's in $GF(p^n)$ such that f(y+z) = f(y) for all y in $GF(p^n)$.

$$\begin{aligned}
0 &= f(y+z)-f(y) \\
&= T\left[\gamma (y+z)^{p^k+1} - (y+z)^{p^{3k}+1} - \gamma y^{p^k+1} + y^{p^{3k}+1}\right] \\
&= T\left[\gamma (y^{p^k}+z^{p^k})(y+z) - (y^{p^{3k}}+z^{p^{3k}})(y+z) - \gamma(y^{p^k}+1) + y^{p^{3k}+1}\right] \\
&= T\left[\gamma (y^{p^k+1} + yz^{p^k} + y^{p^k}z + z^{p^k+1}) - (y^{p^{3k}+1} + yz^{p^{3k}}\right. \\
&\qquad \left. + zy^{p^{3k}} + z^{p^{3k}}) - \gamma(y^{p^k}+1) + y^{p^{3k}+1}\right] \\
&= T\left[\, y^{p^{3k}}\left\{(\gamma z^{p^k})^{p^{3k}} - z^{p^{3k}} \cdot^{p^{3k}} + (\gamma z)^{p^{2k}} - z\right\}\right. \\
&\qquad \left. + \left\{\gamma z^{p^k+1} - z^{p^{3k}+1}\right\}\right]
\end{aligned}$$

Thus, since the above expression must equal zero for all y in $GF(p^n)$, z must be a root of

$$z^{p^{6k}} - \gamma^{p^{3k}} z^{p^{4k}} - \gamma^{p^{2k}} z^{p^{2k}} + z = 0$$

By Proposition 2 of the Appendix there are exactly 1, p^e, or p^{2e} such z's in $GF(p^n)$ where $e = GCD(k,n)$. Hence, the rank of f(y) is n, n-e, or n-2e.

The remainder of the proof is identical to the proof of Theorem 3.3.

Q.E.D.

We can immediately state some simple corollaries. Since

$$p^{2k}-p^k+1 \equiv p^k(p^{n-k} + p^k-1) \pmod{p^n-1}$$

$p^{n-k} + p^k-1$ is in the same cyclotomic coset (mod p^n-1) as $p^{2k}-p^k+1$. Hence,

Corollary: Theorem 3.3 holds with q replaced by $p^{n-k} + p^k - 1$

Consider the following:

$$p^{2k}+1 \equiv p^{2k}+p^n \pmod{p^n-1}$$

$$2(p^{2k}+1) \equiv 2p^{2k}(1-p^{n-2k}) \pmod{p^n-1}$$

$$(p^n+1)(p^{2k}+1) \equiv 2p^{2k}(1+p^{n-2k}) \pmod{p^n-1}$$

$$\frac{p^n+1}{p^{n-2k}+1} \cdot \frac{p^{2k}+1}{2} \equiv p^{2k} \pmod{p^n-1}$$

Hence, $\frac{p^{n+1}}{p^{n-2k+1}}$ and $\frac{p^{2k}+1}{2}$ are in inverse cyclotomic cosets (mod p^n-1). Hence,

Corollary: Theorem 3.3 holds with q replaced by $\frac{p^n+1}{p^{n-2k}+1}$ (mod p^n-1). In particular, for $k = \frac{n-1}{2}$ the division becomes ordinary (mod 0) division since n is odd.

CHAPTER IV

SUMMARY AND REMARKS

IV.A. Summary of Results

We have considered the cross-correlation function of pairs of linear recurring sequences of integers modulo p, p prime, of period $p^n - 1$. We defined the cross-correlation function relative to a mapping χ of GF(p) into the complex numbers. In particular, we considered χ to be the isomorphism of the additive group of GF(p) onto the multiplicative group of complex p^{th} roots of unity. This is the definition of cross-correlation for which the sequences have the well-known two-level autocorrelation property. Although the definition involves a sum of complex numbers, we saw that the cross-correlation assumes real values only.

It was observed that many pairs of sequences have three-level cross-correlation functions. Several theorems and conjectures exist which predict this phenomenon in the case p = 2. In this work, new theorems were proved which predict many of the occurrences of three-level cross-correlation for p an odd prime.

IV.B. Remarks

The proofs of Theorems 3.3 and 3.4 involved the evaluation of $\sum_{x \in GF(p^n)} \chi[f(x)]$ where $\chi[f(x)] = \rho^{f(x)}$, ρ

is a primitive p^{th} root of unity, n is odd, and f(x) is a quadratic form. We saw that the rank of the quadratic form f(x) is n, n-e, or n-2e where e is an odd constant. We observed that when the rank of f(x) is odd, $\sum_{x \in GF(p^n)} \chi \left[f(x)\right] = 0$; and when the rank of f(x) was n-e, the sum equals plus or minus a particular power of p. Suppose, now, that the rank of f(x) could also be n-3e. Then two additional values of $\sum_{x \in GF(p^n)} \chi \left[f(x)\right]$ could occur. We would then have five-level cross-correlation. It would seem, therefore, that the same approach as was taken in Chapter III might lead to theorems which would predict five-level cross-correlation, seven-level correlation, etc. This, however, is not the case. The correlation values which would occur would all be $-1 \pm p^m$ for various integer values of m. However, examination of data revealed that this did not occur except in the three-level case.

Throughout this work we have used a definition of the cross-correlation function of maximal linear sequences which is periodic and which results in constant out of phase autocorrelation. One can define other (perhaps non-periodic) cross-correlation functions. One such definition is

$$C(\tau) = \sum_{i=0}^{p^n-2-\tau} \chi(a_i)\, \chi^*(b_{i+\tau})$$

where once again $\chi(a) = \rho^a$ for ρ a primitive p^{th} root of unity. If $\{b_i\} = \{a_i\}$ and for $\tau \neq 0$, $|C(\tau)| \leq 1$, then one period of $\{a_i\}$ would be a "generalized Barker sequence"

[12] However, one period of a maximal linear sequence does not have this property in general, nor, after inspection of a limited amount of data, does this new definition of cross-correlation in conjunction with maximal linear sequences yield results of any obvious interest.

APPENDIX

Lemma 1: Normal Basic Theorem. There exists an element η in $GF(p^{r \cdot s})$ such that

$$\eta^{p^r}, \eta^{p^{2r}}, \cdots \eta^{p^{sr}} = \eta$$

is a basis of $GF(p^{r \cdot s})$ over $GF(p^r)$. Such a basis is called a normal basis. [13, Theorem 365]

Lemma 2: Let $\zeta_1, \zeta_2, \cdots, \zeta_t$ be a basis of $GF(p^{r \cdot t})$ over $GF(p^r)$. Then there exists a set of elements in $GF(p^{r \cdot t})$--in fact, a basis--say $\gamma_1, \gamma_2, \cdots, \gamma_t$ such that $T[\gamma_i \zeta_j] = \delta_{ij}$ where

$$\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

where T is the trace of $GF(p^{r \cdot t})$ onto $GF(p^r)$. [14, p. 212]

Lemma 3: Let GCD(s,t) = 1. Let $\eta_1, \eta_2, \cdots, \eta_s$ be a normal basis of $GF(p^{r \cdot s})$ over $GF(p^r)$, and let $\zeta_1, \cdots, \zeta_t$ be a basis of $GF(p^{r \cdot t})$ over $GF(p^r)$. Then $\{\eta_i \zeta_j\}$, i = 1, 2, $\cdots$, s, j = 1, $\cdots$, t is a basis for $GF(p^{r \cdot s \cdot t})$ over $GF(p^r)$.

Proof. Suppose not. Then

$$\sum_{i=1}^{s} \sum_{j=1}^{t} a_{ij} \eta_i \zeta_j = 0$$

where $a_{ij} \in GF(p^r)$ and not all the a_{ij} are zero. Let $\{\ell_t\}$ be a set of numbers such that

$$\ell_t \equiv 0 \pmod{t} \text{ and } \ell_t \equiv 0 \pmod{s}$$

$$\ell_1 \equiv 1 \pmod{t} \text{ and } \ell_1 \equiv 0 \pmod{s}$$

$$\vdots$$

$$\ell_{t-1} \equiv t-1 \pmod{t} \text{ and } \ell_{t-1} \equiv 0 \pmod{s}$$

Such numbers exist by the Chinese Remainder Theorem. [15, § 12]

According to Lemma 2, we can pick a set of elements $\{\gamma_k\}$, $k = 1, \cdots, t$, in $GF(p^{rt})$ such that $T[\gamma_k \zeta_j] = \delta_{kj}$ where T is the trace from $GF(p^{rt})$ onto $GF(p^r)$.

Pick a specific k. Since we have assumed

$$\sum_{i=1}^{s} \sum_{j=1}^{t} a_{ij} \eta_i \zeta_j = 0$$

we have

$$0 = \gamma_k \sum_i \sum_j a_{ij} \eta_i \zeta_j$$

$$= \sum_i \sum_j a_{ij} \eta_i \gamma_k \zeta_j$$

$$= \left[\sum_i \sum_j a_{ij} \eta_i \gamma_k \zeta_j\right]^{p^{r\ell_m}}$$

since any power of zero is zero. Summing t terms all equal to zero yields

$$0 = \sum_{m=1}^{t} \left[\sum_{i=1}^{s} \sum_{j=1}^{t} a_{ij} \eta_i \gamma_k \zeta_j \right]^{p^{\ell_m}}$$

Since $a_{ij}^{p} = a_{ij}$ and $\eta_i^{p^s} = \eta_i$ we have

$$0 = \sum_{m} \sum_{i} \sum_{j} a_{ij} \eta_i [\gamma_k \zeta_j]^{p^{r\ell_m}}$$

$$= \sum_{i} \sum_{j} a_{ij} \eta_i \, T[\gamma_k \zeta_j]$$

$$= \sum_{i} \sum_{j} a_{ij} \eta_i \delta_{kj}$$

$$= \sum_{i} a_{ik} \eta_i$$

Hence, $a_{ik} = 0$ for all i. By perfect induction on k we have a contradiction, since $\{\eta_i\}$ i = 1, ···, s is a basis.

Q.E.D.

Lemma 4: Let r, s, and t be pairwise relatively prime. Let $\sigma_1, \sigma_2, \cdots, \sigma_m$, $m \leq s$, be a set of elements of $GF(p^{rs})$ which are linearly independent over $GF(p^r)$. Then $\sigma_1, \sigma_2, \cdots, \sigma_m$ are linearly independent over $GF(p^{rt})$.

Proof. Let $\{\eta_i\} = \{\eta^{p^{ir}}\}$, i = 1,2, ···, s, be a normal basis of $GF(p^{rs})$ over $GF(p^r)$. Let $\{\zeta_j\} = \{\zeta^{p^{jr}}\}$, j=1, ···, t be a normal basis of $GF(p^{rt})$ over $GF(p^r)$.

Since each σ_k is an element of $GF(p^{rs})$, we can write

$$\sigma_k = \sum_{i} a_{ik} \eta_i, \quad a_{ik} \in GF(p^r).$$

An arbitrary element of $GF(p^{rs})$ is $\sum_j b_{kj}\zeta_j$. Therefore, we can express an arbitrary linear combination of σ_k's over $GF(p^{rt})$ as

$$\sum_{k=1}^{m}\sum_{j=1}^{t} b_{kj}\zeta_j \sum_{i=1}^{s} a_{ik}\eta_i$$

$$= \sum_i \sum_j \sum_k a_{ik}b_{ki}\zeta_j\eta_i$$

$$= \sum_i \sum_j c_{ij}\zeta_j\eta_i$$

Since, by Lemma 3, $\{\zeta_j\eta_i\}$ is a basis of $GF(p^{rst})$ over $GF(p^r)$,

$$0 = \sum_i \sum_j c_{ij}\zeta_j\eta_i$$

implies $c_{ij} = 0$ for all i and j. To complete the proof it must be shown that $c_{ij} = 0$ for all i and j implies $b_{kj} = 0$ for all j and each k. But

$$0 = c_{ij}$$

$$= \sum_k a_{ik}b_{kj}$$

$$= \sum_i \eta_i \sum_k a_{ik}b_{kj}$$

$$= \sum_k b_{kj} \sum_i \eta_i a_{ik}$$

$$= \sum_k b_{kj}\sigma_k$$

Hence, $b_{kj} = 0$ for all k and j since the σ_k's are linearly independent over $GF(p^r)$.

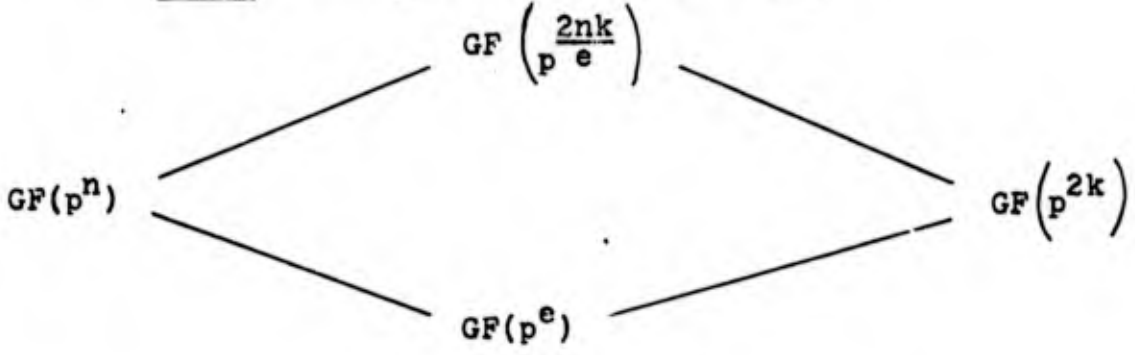
Q.E.D.

Proposition 1: Let be a nonzero element of $GF(p^n)$ where p is prime and n is odd. Then the equation

$$a^{p^{4k}} - (2\gamma)^{p^{2k}} z^{p^{2k}} + z = 0 \qquad (1)$$

has exactly 1, p^e, or p^{2e} roots in $GF(p^n)$, where $e = GCD(k,n)$.

Proof: Consider the tower of fields



Suppose r is an integer which divides s. Let a_1 and a_2 be arbitrary elements of $GF(p^r)$ and let z_1 and z_2 be roots of Eqn. 1 which are also elements of $GF(p^s)$. Then

$$(a_1z_1 + a_2z_2)^{p^s} = (a_1z_1)^{p^s} + (a_2z_2)^{p^s} = a_1z_1^{p^s} + a_2z_2^{p^s}.$$

Thus, the roots of Eqn. 1 which are in $GF(p^s)$ form a linear space over $GF(p^r)$. For the case at hand we consider s = n with r = e and s = 2nk/e with r = 2k.

Suppose that the dimension of the space of roots of Eqn. 1 in $GF(p^n)$ over $GF(p^e)$ is D. Then there are D linearly independent roots of Eqn. 1 in $GF(p^n)$. By Lemma 4 the same D roots are linearly independent over $GF(p^{2k})$, and are a basis of a space of roots of Eqn. 1 in $GF(p^{2nk/e})$ over $GF(p^{2k})$. But since Eqn. has at most $p^{4k} = (p^{2k})^2$ distinct roots, $D \leq 2$.

Q.E.D.

Proposition 2: Let γ be a nonzero element of $GF(p^n)$ where p is an odd prime and n is odd. Then the equation

$$z^{p^{6k}} - \gamma^{p^{3k}} z^{p^{4k}} - \gamma^{p^{2k}} z^{p^{2k}} + z = 0 \qquad (2)$$

has exactly 1, p^e, or p^{2e} roots in $GF(p^n)$, where $e = GCD(k,n)$.

Proof. (Suggested by L. Welch). If a is an element of $GF(p^e)$, then $a^{p^{6k}} = a^{p^{4k}} = a^{p^{2k}} = a$. It is clear, therefore, that the roots of Eqn. 2 in any field of characteristic p form a linear space over $GF(p^e)$.

Let z_1 be a nonzero element of $GF(p^n)$ which is a root of Eqn. 2. (If no such z_1 exists, then Eqn. 2 has exactly one root in $GF(p^n)$--namely, the zero element.)

Let

$$y = z_1^{p^{5k}+p^{2k}} - z_1^{p^{4k}+p^k} + z_1^{p^{3k}+1} - \gamma^{p^{2k}} z_1^{p^{3k}+p^{2k}} \qquad (3)$$

Note that y is an element of $GF(p^n)$ and that

$$y + y^{p^k} = z_1^{p^{5k}} + p^{2k} - z_1^{p^{4k}} + p^k + z_1^{p^{3k}} + 1$$

$$-\gamma^{p^{2k}} z_1^{p^{3k}} + p^{2k} + z_1^{p^{6k}} + p^{3k}$$

$$-z_1^{p^{5k}} + p^{2k} + z_1^{p^{4k}} + p^k - \gamma^{p^{3k}} z_1^{p^{4k}} + p^{3k}$$

$$= z_1^{p^{3k}} \left[z_1^{p^{6k}} - \gamma^{p^{3k}} z_1^{p^{4k}} - \gamma^{p^{2k}} z_1^{p^{2k}} + z_1 \right]$$

$$= 0$$

Since p is odd and $y^{p^k} = -y$ we have

$$y^{p^{2k}} = -(-y)^{p^k} = (-1)^{p^k} y^{p^k} = -(-y) = y.$$

Hence, $y \in GF(p^{2k})$. Since y is also an element of $GF(p^n)$, y must be an element of $GF(p^n) \cap GF(p^{2k}) = GF(p^e)$. But $GF(p^e)$ is a subfield of $GF(p^k)$ and therefore $y \in GF(p^k)$. Hence, $y^{p^k} = y$. Thus $-y = +y$. But for p odd, this implies $y = 0$.

Using Eqn. 3 with $y = 0$ it can be verified by direct expansion that Eqn. 2 can be written

$$(E^2-1)\, z_1^{p^k - p^{2k} + p^{3k}}\, (E^2+1)\, z_1^{1-p^k+p^{2k}}\, (E^2-1)\, z_1^{-1}\, z = 0 \quad (4)$$

where E is the operator defined by $x^E \rightarrow x^{p^k}$.

Suppose now that for some $x \in GF(p^n)$ it is true that

$$(E^2-1)\, z_1^{-1}\, x = 0.$$

We can write $x = z_1 \alpha$ for some $\alpha \in GF(p^n)$. Then

$$(E^2-1)\, z_1^{-1}\, z\alpha = \alpha^{p^{2k}} - \alpha = 0$$

Hence, $\alpha \in GF(p^{2k})$. But $\alpha \in GF(p^n)$ and $\alpha \in GF(p^{2k})$ implies $\alpha \in GF(p^e)$. Thus the rightmost (E^2-1) of Eqn. 4 accounts for p^e roots of Eqn. 4 (including the trivial root) if z_1 exists.

Similarly, the leftmost (E^2-1) in Eqn. 4 annihilates either zero or p^e elements of $GF(p^n)$ which are not annihilated by the operators to the right of it.

Now, consider the operator (E^2+1). If there exists a z in $GF(p^n)$ such that

$$(E^2-1)\, z_1^{-1}\, z \neq 0$$

but

$$(E^2+1)\, x = 0$$

where

$$x = z_1^{1-p^k} + p^{2k}\, (E^2-1)\, z_1^{-1}\, z\ ,$$

then

$$x^{p^{2k}} + x = 0$$

or

$$x^{p^{2k}} = -x.$$

Thus

$$x^{p^{4k}} = (x^{p^{2k}})^{p^{2k}} = (-x)^{p^{2k}} = -x^{p^{2k}} = x.$$

But $x \in GF(p^n)$ and we have just seen that $x \in GF(p^{4k})$. Hence, $x \in GF(p^e)$. Since $GF(p^e)$ is a subfield of $GF(p^{2k})$, $x^{p^{2k}} = x$. We saw above, however, that $x^{p^{2k}} = -x$. Since p is odd, $x = 0$.

It is apparent that the sum of a root annihilated by the rightmost (E^2-1) of Eqn. 4 and a root annihilated by the leftmost (E^2-1) is also a root of Eqn. 2. Hence, there are exactly 1, p^e, or $(p^e)^2 = p^{2e}$ roots of Eqn. 2 in $GF(p^n)$.

Q.E.D.

REFERENCES

1. Golomb, S.W., Shift Register Sequences. San Francisco: Holden-Day, Inc., 1967.

2. Selmer, E. S., "Linear Recurrence Relations Over Finite Fields," University of Bergen, Norway (1966).

3. Zierler, N., "Linear Recurring Sequences," Journal of the Society for Industrial and Applied Mathematics, Vol. 7, No. 1 (March, 1959), pp. 31-48.

4. Gold, R., "Characteristic Linear Sequences and Their Coset Functions," Journal of the Society for Industrial and Applied Mathematics, Vol. 14, No. 5 (September, 1966), pp. 980-985.

5. Gold, R. "Optimum Binary Sequences for Spread-Spectrum Multiplexing," IEEE Transactions on Information Theory, Vol. IT-13, No. 4 (October, 1967), pp. 619-621.

6. Gold, R., "Maximal Recursive Sequences With Three-Valued Recursive Cross-Correlation Function," IEEE Transactions on Information Theory, Vol. 14, No. 1 (January, 1968), pp. 154-156.

7. Welch, L., To appear.

8. Kasami, T., "Weight Distribution Formula for Some Class of Cyclic Codes," Report R-285, Coordinated Science Lab, University of Illinois, Urbana (April, 1966).

9. Solomon, G., and McEleice, R., "Weights of Cyclic Codes," Journal of Combinatorial Theory, Vol. 1, No. 4 (December, 1966), pp. 459-475.

10. Dickson, L.E., Linear Groups with an Exposition of the Galois Field Theory. New York: Dover Publications, Inc., 1958.

11. van der Waerden, B.L., Modern Algebra, Vol. II. New York: Unger Publishing Co., Inc., 1950.

12. Golomb, S.W., and Scholtz, R.A., "Generalized Barker Sequences," IEEE Transactions on Information Theory, Vol. IT-11, No. 4 (October, 1965), pp. 533-537.

13. Redei, L., Algebra, Vol. I. New York: Pergamon Press, 1967.

14. Lang, S., Algebra. Reading, Mass.: Addison-Wesley Publishing Co., Inc., 1965.

15. Dickson, L.E., Introduction to the Theory of Numbers. Chicago: University of Chicago Press, 1929.


USS
Engineering