공학박사 학위논문

Construction of p-ary Sequence Families of Period $(p^n-1)/2$ and Cross-Correlation of p-ary m-Sequences and Their Decimated Sequences

$(p^n-1)/2$ 주기를 가지는 p진 수열군의 생성 및 p진 m-수열의 상호상관도

2015년 2월

서울대학교 대학원

전기·정보공학부

김 지 엽

Construction of p-ary Sequence Families of Period $(p^n-1)/2$ and Cross-Correlation of p-ary m-Sequences and Their Decimated Sequences

지도 교수 노종선

이 논문을 공학박사 학위논문으로 제출함.

2014년 12월

서울대학교 대학원

전기·정보공학부

김 지 엽

김지엽의 공학박사 학위논문을 인준함.

2014년 12월

위 원 장 ______________________ (인)

부위원장 ______________________ (인)

위　　원 ______________________ (인)

위　　원 ______________________ (인)

위　　원 ______________________ (인)

Construction of p-ary Sequence Families of Period $(p^n - 1)/2$ and Cross-Correlation of p-ary m-Sequences and Their Decimated Sequences

Presented to the Graduate School of Seoul National University in Partial Fulfillment of the Requirements for

THE DEGREE OF DOCTOR OF PHILOSOPHY

by

Ji Youp Kim

Department of Electrical and Computer Engineering

Seoul National University

This dissertation approved for

THE DEGREE OF DOCTOR OF PHILOSOPHY

December, 2014

Chairman ____________________

Vice Chairman ____________________

Member ____________________

Member ____________________

Member ____________________

Abstract

Construction of p-ary Sequence Families of Period $(p^n - 1)/2$ and Cross-Correlation of p-ary m-Sequences and Their Decimated Sequences

Ji Youp Kim
Department of ECE
The Graduate School
Seoul National University

This dissertation includes three main contributions: a construction of a new family of p-ary sequences of period $\frac{p^n-1}{2}$ with low correlation, a derivation of the cross-correlation values of decimated p-ary m-sequences and their decimations, and an upper bound on the cross-correlation values of ternary m-sequences and their decimations.

First, for an odd prime $p = 3 \mod 4$ and an odd integer n, a new family of p-ary sequences of period $N = \frac{p^n-1}{2}$ with low correlation is proposed. The family is constructed by shifts and additions of two decimated m-sequences with the decimation factors 2 and $d = N - p^{n-1}$. The upper bound on the maximum value of the magnitude of the correlation of the family is shown to be $2\sqrt{N + 1/2} = \sqrt{2p^n}$ by using the generalized Kloosterman sums. The family size is four times the period of sequences, $2(p^n - 1)$.

Second, based on the work by Helleseth [11], the cross-correlation values between two decimated m-sequences by 2 and $4p^{n/2}-2$ are derived, where p is an odd prime and $n = 2m$ is an integer. The cross-correlation is at most 4-valued and their values are $\{\frac{-1\pm p^{n/2}}{2}, \frac{-1+3p^{n/2}}{2}, \frac{-1+5p^{n/2}}{2}\}$. As a result, for $p^m \neq 2 \mod 3$, a new sequence family with the maximum correlation value $\frac{5}{\sqrt{2}}\sqrt{N}$ and the family size $4N$ is obtained, where $N = \frac{p^n-1}{2}$ is the period of sequences in the family.

Lastly, the upper bound on the cross-correlation values of ternary m-sequences and their decimations by $d = \frac{3^{4k+2}-3^{2k+1}+2}{4} + 3^{2k+1}$ is investigated, where k is an integer and the period of m-sequences is $N = 3^{4k+2} - 1$. The magnitude of the cross-correlation is upper bounded by $\frac{1}{2} \cdot 3^{2k+3} + 1 = 4.5\sqrt{N+1} + 1$. To show this, the quadratic form technique and Bluher's results [33] are employed. While many previous results using quadratic form technique consider two quadratic forms, four quadratic forms are involved in this case. It is proved that quadratic forms have only even ranks and at most one of four quadratic forms has the lowest rank $4k - 2$.

Keywords: Autocorrelation, cross-correlation, decimated sequence, exponential sum, Kloosterman sum, m-sequence, nonbinary sequence, quadratic form, sequence, sequence family

Student ID: 2009-20782

Contents

List of Tables

List of Figures

Chapter 1. Introduction

1.1. Background

Pseudorandom sequences are sequences which are generated in the deterministic way but have similar mathematical and statistical properties of true random sequences. Since they are outputs of some deterministic functions, they can be reproduced when they are needed. Thus, they are extremely useful in the wide range of applications such as signal processing, spread-spectrum communication systems, cryptography, radar systems, global positioning system (GPS), simulations, and more. Therefore, designing good pseudorandom number generators has been important research subject during several decades.

The criterion of "good" pseudorandom sequences depends on the application. Generally in most applications, the cost of pseudorandom sequence generator is an important aspect and thus linear recurrence sequences, which can be efficiently generated by simple linear feedback shift register (LFSR) circuits, are reasonable candidates for the implementation. But in cryptographic applications, LFSR sequences are vulnerable to the plaintext attack [68] and should not be used. Instead, cryptographically secure pseudorandom sequences with the unpredictability property must be employed [76]. A LFSR generator for a sequence of period 15 is shown in Figure 1.1.

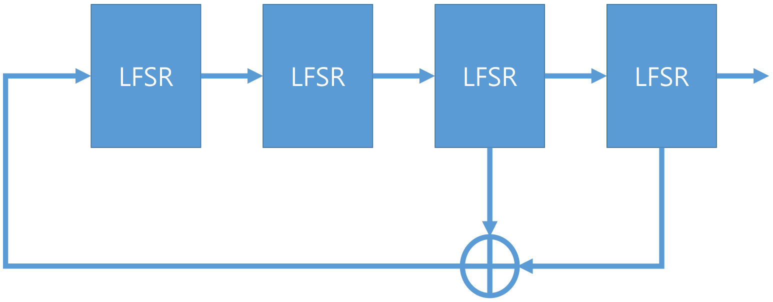

Figure 1.1: LFSR generator of m-sequence with period 15 [74].

Nevertheless, especially for non-cryptographic applications, we can set the general randomness criterion for pseudorandom sequences. For example, in 1955, Golomb [69] proposed the following three randomness postulates for binary sequences [74].

1) Balance property: In every period, the number of zeros is nearly equal to the number of ones.

2) Run property: In every period, half the runs have length 1, one fourth have length 2, one eighth have length 3, and so on, as long as the number of runs so indicated exceeds 1. Moreover, for each of these lengths, there are equally many runs of 0's and 1's.

3) Ideal autocorrelation: The autocorrelation function $C(\tau)$ is two-valued,

given by

$$C(\tau) = \begin{cases} N & \text{if } \tau = 0 \mod N \\ K & \text{if } \tau \neq 0 \mod N, \end{cases}$$

where N is the period of the sequence, $K = -1$ for odd N, and $K = 0$ for even N.

For more general cases including nonbinary sequences and cryptographic applications, we can extend Golomb's three randomness postulates [74].

1) Period requirement: Long period.

2) Statistical properties: The balance property, run property, and ideal k-tuple distribution.

3) Correlation:

   (a) Ideal autocorrelation.

   (b) Low-valued cross-correlation: Let S be a set consisting of finite sequences with period N. For any two sequences a, b in S, the cross-correlation $C_{a,b}(\tau)$ satisfies

   $$0 \leq C_{a,b}(\tau) \leq c\sqrt{N}$$

   where $\tau \neq 0$ when $a = b$, and $c > 0$ is a constant.

4) Linear span: Large ratio of linear span $LS(a)$ to period N,

$$\frac{LS(a)}{N} > \delta,$$

where $\delta > 0$ is a constant for large N.

In some cases, sets of pseudorandom sequences, called sequence families, are considered. In this case, families with large set size or family size are preferred. But there are fundamental tradeoffs between sequence period, nontrivial autocorrelations, cross-correlations, and family size. These tradeoffs are expressed in the form of lower bounds. Welch's lower bound [10] and Sidel'nikov's lower bound [6] are lower bounds for the magnitude of correlation values given the period and the family size. In Levenshtein bound [26], lower bounds for aperiodic correlation magnitudes are given. If these bounds are met with the equalities for some families, then these families of sequences are called optimal.

In this dissertation, we focus on pseudorandom sequences for the spread-spectrum communication systems. In Figure 1.2, the system model for the direct-sequence spread spectrum communication systems is illustrated [75]. First, the message signal is shaped for the baseband transmission. Then the shaped signal is directly multiplied by the spreading sequence, which has the pseudorandom properties. The signal is modulated and transmitted through the channel. After being demodulated in the receiver, the signal is again multiplied by the synchronized spreading sequence. This results in the small inter-user interferences due to the low cross-correlations of spreading sequences. Then the baseband signal is demodulated and the bit decision is made. Thus in this application, the correlation properties of sequences are most important.

There are many good binary pseudorandom sequences. M-sequences

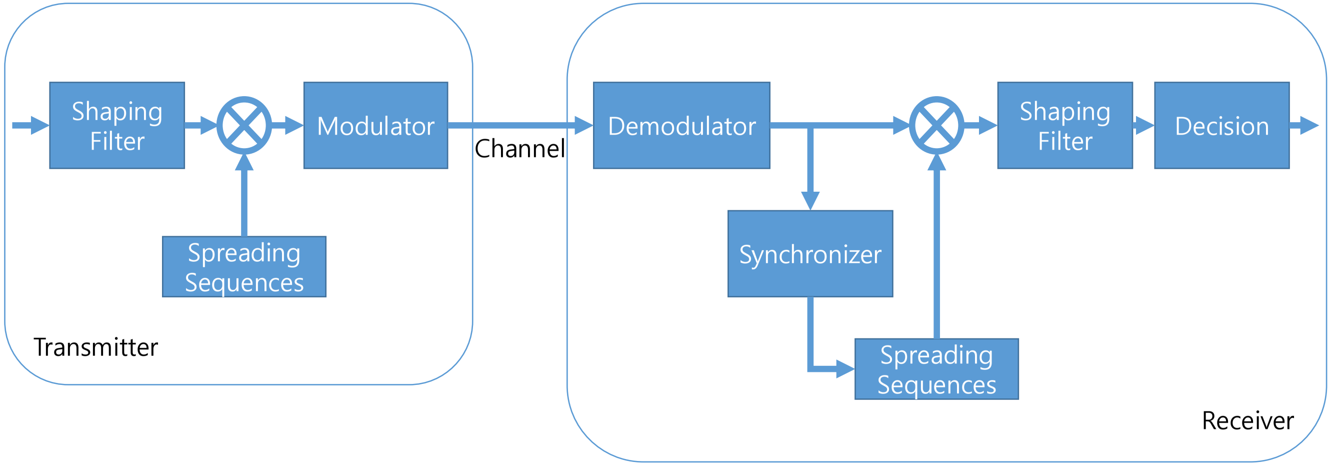

Figure 1.2: Spreading sequences in CDMA communication systems [75].

[69] are the most important one because they satisfy all randomness criterion except the large linear span property. They have elegant mathematical description based on the finite field arithmetic and are efficiently generated by LFSR circuits. Also m-sequences are building blocks for other good pseudorandom sequences. GMW sequences [14] are the generalization of m-sequences and have large linear span and ideal autocorrelation. Legendre sequences [1] are constructed from power residues of the finite field and have ideal autocorrelation. Gold sequences [4] are families of binary sequences constructed from preferred pairs of m-sequences. Kasami sequence families [3] have smaller correlation values than Gold sequence families but have smaller set size. No sequence families [15] generalize GMW sequences and Kasami sequences. Bent function sequences [13] are sequence families based on the bent functions. Kasami, No, and Bent function sequence families are all known to be asymptotically optimal with respect to Welch' lower bound. Besides these, many studies on binary sequences are given [16]-[20] [22].

For nonbinary sequences, m-sequences and GMW sequences can be generalized to p-ary sequences. Liu and Komo [24] extended Kasami sequence families to p-ary alphabets. Kumar and Moreno [23] generalized bent function sequence families to nonbinary case. Based on this, Kim, Jang, No, and Helleseth [30] further generalized p-ary bent function sequences. Sidel'nikov sequences [5] are one of the most important nonbinary sequences and any integer M can be used as the alphabet. Kim, Chung, No, and Chung [31] constructed three families of M-ary sequences using the M-ary Sidel'nikov sequences of period $p^n - 1$. Later, Chung, No, and Chung [45] proposed a family of M-ary sequences with low correlation by the addition of cyclic shifts of an M-ary Sidel'nikov sequence and its reverse sequence. Yu and Gong [39] constructed M-ary sequence families with low correlation using column sequences of the array structure of Sidel'nikov sequences. By combining the methods for generating p-ary extended sequences and p-ary d-form sequences, No [21] presented a construction method of p-ary unified sequences with ideal autocorrelation property. Helleseth and Gong [12] proposed p-ary sequences with ideal autocorrelation called HG sequences. Jang, Kim, No, and Helleseth [32] constructed families of p-ary sequences of period $p^n - 1$ with optimal correlation property. Yu and Gong [40] investigated the Weil bound to construct polyphase sequence families with low correlation. Schmidt [44] proposed nested sequence families using multiplicative and additive characters. Xia [47] constructed families of p-ary sequences from decimated sequences.

There are three main contributions in this dissertation. First, using half-period $\left(N = \frac{p^n-1}{2}\right)$ m-sequences decimated by 2 and $2d = p^n - 1 - 2p^{n-1}$, we have constructed new families of p-ary sequences of period $\frac{p^n-1}{2}$ with low correlation and large family size. The alphabet size p must be an odd prime $p = 3 \mod 4$ and n is an odd integer. The upper bound on the maximum nontrivial correlations between sequences are given as $2\sqrt{N + \frac{1}{2}} = \sqrt{2}p^{n/2}$. The derivation of this bound involved character sums and generalized Kloosterman sums. The maximum magnitude of the correlation is twice of the Welch's lower bound and 1.5 times of the Sidel'nikov's lower bound. The size of the sequence family is $2(p^n - 1) = 4N$, which is four times of the period of sequences. This work has been published in [57] [58].

Second, based on the work bt Helleseth [11], the cross-correlation values between two decimated m-sequences by the decimation factors 2 and $4p^{n/2} - 2$ are derived. Here p is an odd prime and $n = 2m$ is given as an even integer. The cross-correlation functions is shown to be at most 4-valued, that is, $\left\{\frac{-1\pm p^{n/2}}{2}, \frac{-1+3p^{n/2}}{2}, \frac{-1+5p^{n/2}}{2}\right\}$. From this result, for $p^m \neq 2 \mod 3$, new sequence families with family size $4N$ and the maximum correlation magnitude upper bounded by $\frac{-1+5p^{n/2}}{2} \approx \frac{5}{\sqrt{2}}\sqrt{N}$ is constructed, where $N = \frac{p^n-1}{2}$ is the period of sequences in the family. This work will be published as in [60].

Third, we consider the cross-correlation of ternary m-sequences and decimated ternary m-sequences. The period of sequences is $3^n - 1 = 3^{4k+2} - 1$, where k is an integer. The decimation is given as $d = \frac{3^{4k+2} - 3^{2k+1} + 3 - 1}{3+1} + 3^{2k+1}$. For analysis of the correlation, the quadratic form theory is used, and four quadratic forms are involved since we use the substitution $x = y^{3^{n-1}+1}$ and $\gcd(3^n - 1, 3^{n-1} + 1) = 4$ for transforming the correlation into the quadratic forms. To derive the upper bound on the maximum magnitude of the correlation, we have shown that quadratic forms have only even ranks and among four quadratic forms, at most one of them has the lowest rank. In the proof, Bluher's result [33] is proven to be crucial. Consequently, the cross-correlation is upper bounded by $4.5 \cdot 3^{2k+1} + 1$.

This result was presented in [59].

1.2. Overview of Dissertation

This dissertation is organized as follows. In Chapter 2, we briefly overview basic concepts of pseudorandom sequences. Some necessary definitions and preliminaries for sequence analysis are given. Then we consider sequences with low autocorrelation, and introduce some well-known sequences with ideal autocorrelation. After that, sequence families with low correlation are discussed shortly.

In Chapter 3, we propose a new family of p-ary sequences of period $\frac{p^n-1}{2}$ with low correlation and large family size. For this, we introduce definitions and basic facts of characters, Gaussian sums, Kloosterman sums, and generalized Kloosterman sums. Using these exponential sums, we show that the sequence family has the maximum correlation bound $2\sqrt{N+\frac{1}{2}}$ where N is the period of sequences.

In Chapter 4, for an odd prime p and an even integer $n = 2m$, the cross-correlation function between two p-ary m-sequences decimated by 2 and $d' = 4p^{n/2} - 2$ are considered. This decimation is based on the work by Helleseth [11], and we show that the number of the cross-correlation is at most four and possible correlation values are $\frac{-1\pm p^{n/2}}{2}$, $\frac{-1+3p^{n/2}}{2}$, and $\frac{-1+5p^{n/2}}{2}$. From this, for $p^m \neq 2 \mod 3$, a new family of p-ary sequences of period $\frac{p^n-1}{2}$ with low correlation and large family size is constructed. The maximum magnitude of correlation is upper bounded by $\frac{-1+5p^{n/2}}{2}$ and the family size is $4N$.

In Chapter 5, we study the cross-correlation between ternary m-sequences and their decimated sequences by $d = \frac{3^{4k+2}-3^{2k+1}+3-1}{3+1} + 3^{2k+1}$, where the period of sequences is given as $3^{4k+2} - 1$. We derive the upper bound on the cross-correlation and the quadratic form technique is used as the main tool of analysis. In this work, four quadratic forms are considered and rank combinations of quadratic forms are investigated. Bluher's work [33] turns out to be essential in this approach.

Finally, in Chapter 6, the concluding remarks are given.

Chapter 2. Sequences with Low Correlation

In this chapter, we introduce some necessary notations and definitions. First, we define the trace function, sequences, and autocorrelation of sequences. Then we define the ideal autocorrelation property and discuss several known sequences with ideal autocorrelation. Later, the definition of sequence families is introduced, and the tradeoffs between the sequence period, the family size, and the maximum correlation magnitude are discussed. Finally we explain the decimation of sequences and show that the sequence family can be constructed by the shift-and-add method and the decimation.

2.1. Trace Functions and Sequences

Sequences with low correlation can be constructed in various ways. But many sequences with good correlation properties are defined in terms of the *trace function.* The trace function is a mapping defined on the finite field and the trace representation of sequences enables easy analysis of pseudorandom sequences. The precise definition of the trace function is given below.

Definition 2.1. Let p be a prime and n, m be integers such that $m|n$. Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements. Then the trace function

$\mathrm{tr}_n^m(x) : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is defined as

$$\mathrm{tr}_m^n(x) = \sum_{i=0}^{n/m-1} x^{p^{im}}$$

where $x \in \mathbb{F}_{p^n}$. □

The trace function has many important properties. Some of them are summarized as in the following [71].

Lemma 2.2. The trace function satisfies

(1) $\mathrm{tr}_m^n(ax+by) = a\mathrm{tr}_m^n(x)+b\mathrm{tr}_m^n(y)$, for all $a, b \in \mathbb{F}_{p^m}$ and all $x, y \in \mathbb{F}_{p^n}$.

(2) $\mathrm{tr}_m^n(x^{p^m}) = \mathrm{tr}_m^n(x)$ for all $x \in \mathbb{F}_{p^n}$.

(3) Let k, m, n be integers such that $k|m|n$. Then we have

$$\mathrm{tr}_k^n(x) = \mathrm{tr}_k^m(\mathrm{tr}_m^n(x)), \text{ for all } x \in \mathbb{F}_{p^n}.$$

(4) For any $b \in \mathbb{F}_{p^m}$, it holds that

$$|\{x \in \mathbb{F}_{p^n} | \mathrm{tr}_m^n(x) = b\}| = p^{n-m}.$$

(5) Let $a \in \mathbb{F}_{p^n}$. If $\mathrm{tr}_m^n(ax) = 0$ for all $x \in \mathbb{F}_{p^n}$, then $a = 0$. □

A sequence is a function $s(t)$ from the set of natural numbers $\mathbb{N}$ to A where A is a set. In this case, A is called an *alphabet* of $s(t)$. If $A = \mathbb{Z}_M$, then $s(t)$ is an M-ary sequence.

The *autocorrelation* is one of the most important metric of the randomness of sequences. The autocorrelation of a sequence is the measure of similarity between the sequence and its shifted version and is defined as follows.

Definition 2.3. Let $s(t)$ be an M-ary sequence of period N. Then we define the autocorrelation $C_s(\tau)$ of $s(t)$ as

$$C_s(\tau) = \sum_{t=0}^{N-1} \omega_M^{s(t+\tau)-s(t)}$$

where ω_M is the primitive M-th root of unity, i. e., $e^{j2\pi/M}$, and $t+\tau$ is computed $\bmod N$. □

When $\tau \neq 0$, then we call $C_s(\tau)$ the nontrivial autocorrelation.

A sequence is *balanced* if the number of occurrences of each symbol differs by at most one [74]. Also a sequence satisfies the *ideal k-tuple distribution* if for $1 \leq j \leq k$, each of the j-tuples occurs equally many times except one choice of j-tuple in one period [14]. These properties are the measure of the uniformity of sequence values.

A *linear complexity* is particularly important for the cryptographic application since it is the measure of the unpredictability. Linear complexity is defined to be the minimal number of LFSRs for generating the sequence. Generally, if the linear complexity of the sequence is comparable to the period, then it is considered to be sufficiently large [74].

2.2. Sequences with Low Autocorrelation

Sequences with low autocorrelation can be easily distinguished from its shifted version. Thus, sequences with small autocorrelation are employed in radar systems, synchronization, ranging systems, and so forth. If the nontrivial autocorrelation of a sequence is always zero, then the sequence is called *perfect sequence*. It is the best autocorrelation property, but in

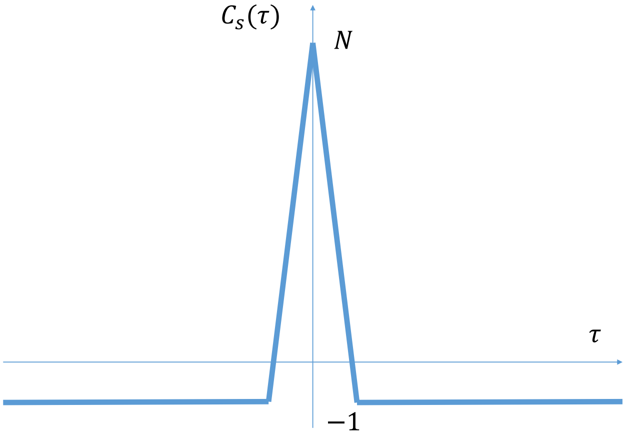

Figure 2.1: Ideal autocorrelation property.

many cases, perfect autocorrelation property is not possible. For example, for an odd prime p and an integer n, a p-ary sequence of period $p^n - 1$ cannot be perfect. Instead, we define the *ideal autocorrelation* as follows.

Definition 2.4. For a prime p, a p-ary sequence $s(t)$ has the ideal autocorrelation if

$$C_s(\tau) = \begin{cases} N & \text{if } \tau = 0 \mod N \\ -1 & \text{otherwise} \end{cases}$$

where N is period of $s(t)$. □

The ideal autocorrelation is presented in Figure 2.1. Note that the resemblance between the autocorrelation of the white noise and that of the sequence with ideal autocorrelation.

There are many sequences with ideal autocorrelation. Among them, *m-sequences* are the most important. The "m" refers the maximum length because m-sequences are the longest sequences given the same number of

LFSRs. The definition of m-sequences are given below.

Definition 2.5. Let p be an odd prime and let n be an integer. Then, m-sequence $m(t)$ of period $p^n - 1$ is defined as

$$m(t) = \mathrm{tr}_1^n(\alpha^t)$$

where α is a primitive element of the finite field $\mathbb{F}_{p^n}$. □

M-sequences have many desirable properties. They have the largest possible period $p^n - 1$ and the ideal autocorrelation property. They also satisfy the balance property, the n-tuple distribution property, and the run property. Major drawback of m-sequences is small linear complexity. They have linear complexity n, which is significantly small compared to the period $p^n - 1$. Therefore, m-sequences are inappropriate for cryptographic applications.

Another important sequence with ideal autocorrelation is the *GMW sequence.* It has large linear complexity compared with the m-sequence.

Definition 2.6 (Scholtz and Welch [14])**.** Let p be an odd prime and let n, m be an integer satisfying $m|n$. Let r be integers with $1 \leq r \leq p^m - 2$ and $\gcd(r,\ p^n - 1) = 1$. Then, GMW sequence $g(t)$ of period $p^n - 1$ is defined as

$$g(t) = \mathrm{tr}_1^m(\{\mathrm{tr}_m^n(\alpha^t)\}^r)$$

where α is a primitive element of the finite field $\mathbb{F}_{p^n}$. □

Helleseth and Gong [12] constructed the following p-ary sequences with ideal autocorrelation. They are called *HG sequences.*

Theorem 2.7 (Helleseth and Gong [12])**.** Let α be a primitive element of $\mathbb{F}_{p^n}$. Let $n = (2m + 1)k$ and let $s, 1 \leq s \leq 2m$ be an integer such that

$\gcd(s,\ 2m+1) = 1$. Define $b_0 = 1, b_{is} = (-1)^i$, and $b_i = b_{2m+1-i}$ for $i = 1, 2, ..., m$. Let $u_0 = b_0/2 = (p+1)/2$ and $u_i = b_{2i}$ for $i = 1, 2, ..., m$. Let $q = p^k$. Define

$$f(x) = \sum_{i=0}^{m} u_i x^{(q^{2i}+1)/2}$$

or

$$f(x) = \sum_{i=0}^{m-i} u_i x^{(q^{2i+1}+1)/(q+1)}.$$

Then the sequences defined by

$$s(t) = \mathrm{tr}_1^n(f(\alpha^t))$$

has the ideal autocorrelation, where all indices of the b_i's are taken modulo $2m+1$. □

No [21] introduced *p-ary unified sequences*, which are very general class of p-ary sequences including the binary and nonbinary extended sequences and the d-form sequences.

Theorem 2.8 (No [21])**.** Let p be a prime number, m, n be positive integers such that $m|n$. Define $N = p^n - 1, M = p^m - 1$, and $T = N/M = (p^n - 1)/(p^m - 1)$. Let α be a primitive element of $\mathbb{F}_{p^n}$ and $\beta = \alpha^T$. Assume that for an index set I, the sequence $b_u(t_1)$ of period M given by

$$b_u(t_1) = \sum_{a \in I} b_a \mathrm{tr}_1^m(\beta^{at_1}), b_a \in \mathbb{F}_p^*$$

has the ideal autocorrelation property. Let $s = d \mod M$ for all s in some index set J, where d is relatively prime to M. Assume that the p-ary sequence $c(t)$ of period N given by

$$c(t) = \sum_{s \in J} c_s \mathrm{tr}_1^n(\alpha^{st}), c_s \in \mathbb{F}_p^*$$

has the ideal autocorrelation property. For an integer r, $1 \le r \le M-1$, relatively prime to M, the unified sequence $c_u(t)$ of period N defined by

$$c_u(t) = \sum_{a \in I} b_a \mathrm{tr}_1^m \left\{ \left[\sum_{s \in J} c_s \mathrm{tr}_m^n(\alpha^{st}) \right]^{ar} \right\}$$

also has the ideal autocorrelation property. □

In 1998, Lin [25] proposed a conjecture that a class of ternary sequences has the ideal autocorrelation property. Arasu, Dillon, and Player [41] and Hu, Shao, Gong, and Helleseth [28], using different methods, proved that the conjecture is true. We introduce the result here.

Theorem 2.9 (Lin [25], Arasu, Dillon, and Player [41], Hu, Shao, Gong, and Helleseth [28])**.** Let $n = 2m+1$ and m be integers. Let α be a primitive element of $\mathbb{F}_{3^n}$. Then a sequence defined by

$$s(t) = \mathrm{tr}_1^n(\alpha^t + \alpha^{(2\cdot 3^m+1)t})$$

has the ideal autocorrelation. □

2.3. Sequence Families with Low Correlation

A set of sequences is called a family of sequences or a sequence family. Usually we deal with the sequence family within which all sequences have the same length and the same alphabet. The set size of the sequence family is called the family size. Here we only count sequences which are cyclically inequivalent, that is, only those sequences $a(t), b(t)$ such that $a(t+\tau) \neq b(t)$ for all $0 \le \tau < N$, where N is the period of sequences. The cross-correlation between sequences $a(t)$ and $b(t)$ is defined as follows.

Definition 2.10. Let $a(t)$, $b(t)$ be M-ary sequences of period N. Then the cross-correlation $C_{a,b}(\tau)$ of $a(t)$, $b(t)$ at time shift τ is defined as

$$C_{a,b}(\tau) = \sum_{t=0}^{N-1} \omega_M^{a(t+\tau)-b(t)}$$

where ω_M is the primitive M-th root of unity, i.e., $e^{j2\pi/M}$, and $t+\tau$ is computed $\mod N$. □

The primary metric of the sequence family is the maximum magnitude of correlation which is defined as in the following definition.

Definition 2.11. Let S be a sequence family. The maximum magnitude of correlation $C_{max}(S)$ is given as

$$C_{max}(S) = \max\{|C_{a,b}(\tau)||a, b \in S, a \neq b \text{ or } \tau \neq 0\}.$$

□

If $C_{max}(S) \leq c\sqrt{N} + d$ for a constant c, d and the period N, then we say that S has low correlation. In general, smaller correlation and larger family size are desirable. But for the given period, the maximum correlation magnitude and the family size have the fundamental tradeoff. This tradeoff is described by several lower bounds on the cross-correlation magnitude. Here we introduce two of such bounds, *Welch's lower bound* [10] and *Sidel'nikov's lower bound* [6].

Theorem 2.12 (Welch [10])**.** Let S be the sequence family with sequences of period N and family size M. Then for any $a, b \in S$ and $0 \leq \tau < N$, we have

$$|C_{a,b}(\tau)| \geq \sqrt{\frac{1}{M-1}\left[\frac{MN^2}{N} - N^2\right]}.$$

□

Theorem 2.13 (Sidel'nikov [6]). Let S be the sequence family of period N and family size M. Let $a, b \in S$ and $0 \leq \tau < N$. In the case of $M = 2$, then we have

$$|C_{a,b}(\tau)| \geq \sqrt{(2k+1)(n-k) + \frac{k(k+1)}{2} - \frac{2^k N^{2k+1}}{M(2k)!\binom{n}{k}}}, 0 \leq k\frac{2N}{5}.$$

In the case of $M > 2$, then we have

$$|C_{a,b}(\tau)| \geq \sqrt{\frac{k+1}{2}(2n-k) - \frac{2^k N^{2k+1}}{M(k!)^2\binom{2n}{k}}}, k \geq 0.$$

□

For a sequence $s(t)$ of period N and an integer d, the decimated sequence of $s(t)$ by the decimation d is defined as $s(dt)$. Note that the period of the decimated sequence is $N/\gcd(d, N)$. Thus decimation yields a short period sequence. Many sequence families can be constructed using m-sequences and decimated m-sequences. For example, *Gold sequence family* [4] is constructed by the shift-and-add method and the decimation.

Definition 2.14 (Gold [4]). Let n, k be integers such that

$$\gcd(n, k) = \begin{cases} 1, \text{for } n \text{ odd} \\ 2, \text{for } n = 2 \mod 4. \end{cases}$$

Let $d = 2^k + 1$ or $d = 2^{2k} - 2^k + 1$. Let $m(t)$ be a binary m-sequence of period $N = 2^n - 1$. Then Gold sequence family is defined as

$$S = \{s_i(t) | 0 \leq t \leq N-1, 0 \leq i \leq N+1\}$$

where $s_i(t) = m(t) + m(dt + i)$, $0 \leq i \leq N-1$, $s_N(t) = m(t)$, and $s_{N+1}(t) = m(dt)$. □

The Gold sequence family is known to be optimal for odd n with respect to the Sidel'nikov's lower bound. Its correlation values are

$$\{-2^{\frac{n+1}{2}}-1,-1,2^{\frac{n+1}{2}}-1\} \text{ for odd } n$$

$$\{-2^{\frac{n+2}{2}}-1,-1,2^{\frac{n+2}{2}}-1\} \text{ for even } n.$$

Many other sequence families are constructed by the shift-and-add method. In this dissertation, we will propose new families of sequences of period $\frac{p^n-1}{2}$ with low correlation.

Chapter 3. A New Family of p-ary Sequences of Period $(p^n - 1)/2$ with Low Correlation

In this chapter, for an odd prime p congruent to 3 modulo 4 and an odd integer n, a new family of p-ary sequences of period $N = \frac{p^n-1}{2}$ with low correlation is proposed. The family is constructed by shifts and additions of two decimated m-sequences with the decimation factors 2 and $2d$, $d = N - p^{n-1}$. The upper bound on the maximum magnitude of nontrivial correlations of this family is derived using well known Kloosterman sums. The upper bound is shown to be $2\sqrt{N + \frac{1}{2}} = \sqrt{2p^n}$, which is twice the Welch's lower bound and approximately 1.5 times the Sidel'nikov's lower bound. The size of the family is $2(p^n - 1)$, which is four times the period of sequences.[1]

[1] The material of this chapter is primarily based on the following paper and proceeding: ©2010 IEEE. Reprinted, with permission, from Ji-Youp Kim, Sung-Tai Choi, Jong-Seon No, and Habong Chung, "A new family of p-ary decimated sequences with low correlation," *IEEE International Symposium on Information Theory*, Austin, TX, Jun. 2010 and ©2011 IEEE. Reprinted, with permission, from Ji-Youp Kim, Sung-Tai Choi, Jong-Seon No, and Habong Chung, "A new family of p-ary sequences of period $(p^n - 1)/2$ with low correlation," *IEEE Transactions on Information Theory*, vol. 57, no. 6, pp. 3825-3830, Jun. 2011.

3.1. Introduction

Many families of pseudorandom sequences have been reported to have good correlation properties. Gold sequence family has low cross-correlation and large family size [4]. Kasami sequence family [2] [3] has lower cross-correlation than that of Gold, but it has smaller family size. Gold and Kasami sequence families are optimal with respect to the Sidel'nikov's and the Welch's lower bounds, respectively. Besides these binary sequence families, there have been many researches on nonbinary sequence families. Liu and Komo [24] generalized Kasami sequence family to nonbinary case. Helleseth [11] investigated into various cross-correlations between m-sequences and their decimations. From these results, p-ary sequence families of period $p^n - 1$, the maximum correlation bound $1 + 2\sqrt{p^n}$, and family size $p^n + 1$ has been constructed [23]. Based on the result of Trachenberg [7], a nonbinary sequence family with the maximum correlation bound $1 + \sqrt{p^{n+1}}$ and family size $p^n + 1$ is obtained [23]. Kumar and Moreno [23] designed an asymptotically optimal family with the correlation upper bound $1 + \sqrt{p^n}$.

More recently, Kim, Chung, No, and Chung [31] constructed M-ary sequence families from Sidel'nikov sequences. Han and Yang [38] proposed M-ary sequence families having the same upper bound on the maximum correlation magnitudes, but larger family size. Yu and Gong [40] refined the Weil bound to construct polyphase sequence families including some known families in [38] as a special case. They also presented the array structure of M-ary Sidel'nikov sequences and constructed M-ary sequence families with low correlation from column sequences of the array structure in [40]. Schmidt [44] proposed nested families of polyphase sequences which have prime period.

This chapter presents a new construction of a p-ary sequence family with low correlation. For a prime p of 3 mod 4 and an odd integer n, a new p-ary sequence family of period $\frac{p^n-1}{2}$ having the maximum correlation magnitude $\sqrt{2p^n}$ is constructed. This maximum correlation magnitude is asymptotically twice the Welch's lower bound and 1.5 times the Sidel'nikov's lower bound, but its family size is four times the period of sequences. This family can be obtained from shifts and additions of two decimated p-ary m-sequences by 2 and $2d$, $d = \frac{p^n-1}{2} - p^{n-1}$, and the size of the family is $2(p^n - 1)$.

This chapter is organized as follows. In Section 3.2, we introduce the concept of characters and give definitions of additive characters and multiplicative characters. Next in Section 3.3, Gaussian sums, Kloosterman sums, and generalized Kloosterman sums are defined, and related lemmas are reviewed. In Section 3.4, notations used throughout this chapter are collected. In Section 3.5, the construction of the sequence family is given. The upper bound on the maximum magnitude of correlation of the sequence family is proved in Section 3.6. The family size is discussed in Section 3.7. An example of the family is given in Section 3.8. Some generalization of this work by Kim, Chae, and Song [61] is introduced in Section 3.9. Finally, we conclude this chapter in Section 3.10.

3.2. Characters

In this chapter, character sums are used for computation of the correlation. Generally, the character is defined as follows [72] [73].

Definition 3.1 (Characters [72] [73])**.** Let G be a finite group and $\mathbf{GL}_m(\mathbb{C})$ be a general linear group of degree m over the complex field. Let $\phi : G \to \mathbf{GL}_m(\mathbb{C})$ be a group homomorphism. Then the function $f = \mathrm{tr} \circ \phi : G \to \mathbb{C}$

$$f(x) = \mathrm{tr}(\phi(x)), g \in G$$

is called a character. □

In this section, we consider two different characters. The first one is an additive character, in which $G = \mathbb{F}_{p^n}$ is an additive group and $m = 1$, i.e., $\mathbf{GL}_m(\mathbb{C}) = \mathbb{C}^* = \mathbb{C} \backslash \{0\}$. The precise definition of the additive character is given as follows.

Definition 3.2 (Additive characters [70])**.** Let p be a prime number and n be an integer. The additive character χ is a group homomorphism

$$\chi : \mathbb{F}_{p^n} \to \mathbb{C}^*.$$

In particular, the canonical character χ_1 is given as

$$\chi_1(x) = e^{\frac{2\pi\sqrt{-1}}{p}\mathrm{tr}_1^n(x)}$$

where $x \in \mathbb{F}_{p^n}$. □

It is known that any additive character can be expressed as $\chi_a(x) = \chi_1(ax)$ for some $a \in \mathbb{F}_{p^n}$. Trivial additive character χ_0 is a character which maps every element of $\mathbb{F}_{p^n}$ into 1. The conjugate character of χ is the character such that $\bar{\chi}(x) = \overline{\chi(x)}$, where $\bar{()}$ denotes complex conjugate.

The second one is a multiplicative character, in which $G = \mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \backslash \{0\}$ is a multiplicative group and $m = 1$, i.e., $\mathbf{GL}_m(\mathbb{C}) = \mathbb{C}^* = \mathbb{C}\backslash\{0\}$. The multiplicative character is defined as follows.

Definition 3.3 (Multiplicative characters [70])**.** Let p be a prime number and n be an integer. The multiplicative character ψ is a group homomorphism

$$\psi : \mathbb{F}_{p^n}^* \to \mathbb{C}^*.$$

Every multiplicative character can be given as

$$\psi_j(\alpha^k) = e^{\frac{2\pi\sqrt{-1}jk}{p^n-1}}$$

for some $0 \leq j, k < p^n - 1$. □

Here ψ_0 is called a trivial multiplicative character. Conjugate characters of multiplicative characters are defined similarly as in the case of additive characters.

The multiplicative character of the particular importance is the quadratic character. It is defined as follows.

Definition 3.4 (Quadratic characters [70])**.** Let p be a prime number and n be an integer. The quadratic character η is given as

$$\eta(x) = \begin{cases} 1, & \text{if } x \text{ is a nonzero square in } \mathbb{F}_{p^n} \\ -1, & \text{if } x \text{ is a nonzero nonsquare in } \mathbb{F}_{p^n}. \end{cases}$$

□

3.3. Gaussian Sums and Kloosterman Sums

Gaussian sums and Kloosterman sums are two important classes of the exponential sums. They are useful to represent the correlation function by the exponential sum. First we give the definition of Gaussian sums.

Definition 3.5 (Gaussian sums [70]). Let ψ be a multiplicative character and χ be an additive character. Then the Gaussian sum $G(\psi, \chi)$ is defined as

$$G(\psi, \chi) = \sum_{c \in \mathbb{F}_{p^n}^*} \psi(c)\chi(c).$$

□

The following lemmas for the Gaussian sum are needed for proof of the main theorem of this chapter.

Lemma 3.6 (Theorem 5.11 [70]). Let ψ be a multiplicative character and χ an additive character of $\mathbb{F}_{p^n}$. Then the Gaussian sum $G(\psi, \chi)$ satisfies

$$G(\psi, \chi) = \begin{cases} p^n - 1 & \text{for } \psi = \psi_0 \text{ and } \chi = \chi_0 \\ -1 & \text{for } \psi = \psi_0 \text{ and } \chi \neq \chi_0 \\ 0 & \text{for } \psi \neq \psi_0 \text{ and } \chi = \chi_0 \end{cases}$$

and

$$|G(\psi, \chi)| = \sqrt{p^n} \quad \text{for } \psi \neq \psi_0 \text{ and } \chi \neq \chi_0.$$

□

Now we define the Kloosterman sum as follows.

Definition 3.7 (Kloosterman sums [70]). Let a and b be elements of $\mathbb{F}_{p^n}$ and χ be an additive character of $\mathbb{F}_{p^n}$. Then the Kloosterman sum

$K(\chi; a, b)$ is defined as

$$K(\chi; a, b) = \sum_{y \in \mathbb{F}_{p^n}^*} \chi(ay + by^{-1}).$$

□

In the proof of the main theorem, we need the upper bound on the Kloosterman sum. We can use the following well-known upper bound.

Lemma 3.8 (Theorem 5.45 [70])**.** If χ is a nontrivial additive character of $\mathbb{F}_{p^n}$ and $a, b \in \mathbb{F}_{p^n}$ are not both 0, then the Kloosterman sum $K(\chi; a, b)$ satisfies

$$|K(\chi; a, b)| \leq 2\sqrt{p^n}.$$

□

Note that contrary to Gaussian sums, Kloosterman sums only involve additive characters. The Kloosterman sum can be generalized to include a multiplicative character.

Definition 3.9 (Generalized Kloosterman sums [70])**.** Let ψ be a multiplicative character and χ an additive character of $\mathbb{F}_{p^n}$. For $a, b \in \mathbb{F}_{p^n}$, a generalized Kloosterman sum is defined as

$$K(\psi, \chi; a, b) = \sum_{y \in \mathbb{F}_{p^n}^*} \psi(y)\chi(ay + by^{-1}).$$

□

Many results are reported for the Gaussian and the Kloosterman sums. Here we list some of them which are used in this chapter.

Lemma 3.10 (Exercise 5.83 [70])**.** Let ψ be a multiplicative character and χ an additive character of $\mathbb{F}_{p^n}$. The generalized Kloosterman sum reduces to a Gaussian sum if $ab = 0$, in the sense that

$$K(\psi, \chi; a, b) = \begin{cases} \psi(b)G(\bar{\psi}, \chi) & \text{if } a = 0, b \neq 0 \\ \bar{\psi}(a)G(\psi, \chi) & \text{if } a \neq 0, b = 0 \\ G(\psi, \chi_0) & \text{if } a = 0, b = 0. \end{cases}$$

□

Lemma 3.11 (Exercise 5.84 [70])**.** Let η be the quadratic character of $\mathbb{F}_{p^n}$, p an odd prime, and $a, b \in \mathbb{F}_{p^n}$ with $\eta(ab) = -1$. Then we have

$$K(\eta, \chi; a, b) = 0$$

for any additive character χ of $\mathbb{F}_{p^n}$. □

Lemma 3.12 (Exercise 5.85 [70])**.** Let η be the quadratic character of $\mathbb{F}_{p^n}$, p an odd prime, and $a, b \in \mathbb{F}_{p^n}$ with $ab = e^2$ for some $e \in \mathbb{F}_{p^n}^*$. Then we have

$$K(\eta, \chi; a, b) = \eta(b)G(\eta, \chi)(\chi(2e) + \chi(-2e))$$

for any additive character χ of $\mathbb{F}_{p^n}$. □

3.4. Notations

Here we collect notations used in this chapter.

- p is an odd prime (3 mod 4);
- n is an odd positive integer;
- $N = \frac{p^n-1}{2}$;
- $d = N - p^{n-1}$;
- α is a primitive element of $\mathbb{F}_{p^n}$;

- ω is a primitive p-th root of unity;

- $QR = \{a \in \mathbb{F}_{p^n}^* | x^2 = a$ has a solution in $\mathbb{F}_{p^n}\}$;

- $QNR = \{a \in \mathbb{F}_{p^n}^* | x^2 = a$ has no solution in $\mathbb{F}_{p^n}\}$.

3.5. Definition of Sequence Family

In this section we present the construction method of the sequence family. Let $m(t)$ be an m-sequence of period $p^n - 1$. Since $p^n - 1$ is even, the decimated sequence $s(2t)$ has the period $N = (p^n - 1)/2$. In order to construct the sequence family, the sequence $m(2t)$ and its decimated sequence $m(2dt)$ are considered. Since $\gcd(N, d) = 1$, the period of $m(2dt)$ is also N.

The family S of our interest is defined as

$$\mathcal{S} = \bigcup_{j=1}^{4} \mathcal{S}_|$$

where

$$\mathcal{S}_\infty = \{m(2t) + m(2d(t+j))|0 \leq j < N\}$$

$$\mathcal{S}_\in = \{m(2t+1) + m(2d(t+j))|0 \leq j < N\}$$

$$\mathcal{S}_\ni = \{m(2t) + m(2d(t+j)+1)|0 \leq j < N\}$$

$$\mathcal{S}_\triangle = \{m(2t+1) + m(2d(t+j)+1)|0 \leq j < N\}.$$

In the following section, we will show that the magnitude of cross-correlation and nontrivial autocorrelation values of the p-ary sequences in $\mathcal{S}$ are upper bounded by $2\sqrt{N + \frac{1}{2}} = \sqrt{2p^n}$.

3.6. Correlation Bound

The upper bound on the correlation magnitude of the sequence family $\mathcal{S}$ is derived in the main theorem. For the proof of the main theorem, we need the following lemma.

Lemma 3.13. For a and $b \in \mathbb{F}_{p^n}$, let $L(\chi_1; a, b)$ be defined as

$$L(\chi_1; a, b) = \sum_{y \in \mathbb{F}_{p^n}^*} \eta(y) \omega^{\mathrm{tr}_1^n(ay+by^{-1})}$$

where η is the quadratic character. Then we have

$$|L(\chi_1; a, b)| \leq 2\sqrt{p^n}.$$

Proof. We consider the following three cases:
i) $ab = 0$;
In this case, we can use Lemma 3.10. Since $|\eta(x)| \leq 1$ for any $x \in \mathbb{F}_{p^n}$, we have

$$\begin{aligned} |L(\chi_1; a, b)| &= \Big| \sum_{y \in \mathbb{F}_{p^n}^*} \eta(y) \omega^{\mathrm{tr}_1^n(ay+by^{-1})} \Big| \\ &= |K(\eta, \chi_1; a, b)| \\ &\leq \begin{cases} |G(\bar{\eta}, \chi_1)| & \text{if } a = 0, b \neq 0 \\ |G(\eta, \chi_1)| & \text{if } a \neq 0, b = 0 \\ |G(\eta, \chi_0)| & \text{if } a = 0, b = 0. \end{cases} \end{aligned}$$

Since η is not trivial, Lemma 3.6 indicates that

$$|L(\chi_1; a, b)| \leq \sqrt{p^n}.$$

ii) $ab \in QR$;
Here $ab = e^2$ for some $e \in \mathbb{F}_{p^n}^*$. Then by applying Lemma 3.12, we have

$$|L(\chi_1; a, b)| = |K(\eta, \chi_1; a, b)|$$

$$
\begin{aligned}
&= |\eta(b)G(\eta,\chi_1)(\chi_1(2e)+\chi_1(-2e))| \\
&\le 2|G(\eta,\chi_1)| \\
&\le 2\sqrt{p^n}.
\end{aligned}
$$

iii) $ab \in QNR$;
Using $\eta(ab) = -1$ and Lemma 3.11, we have

$$
\begin{aligned}
|L(\chi_1;a,b)| &= |K(\eta,\chi_1;a,b)| \\
&= 0.
\end{aligned}
$$

Therefore, for any $a, b \in \mathbb{F}_{p^n}$, we have

$$|L(\chi_1;a,b)| \le 2\sqrt{p^n}.$$

□

Now we are ready to prove the main theorem of this chapter.

Theorem 3.14. The magnitudes of cross-correlation and nontrivial autocorrelation values of sequences in $\mathcal{S}$ are upper bounded by $2\sqrt{N+\frac{1}{2}}$.

Proof. First we consider the cross-correlation of sequences in $\mathcal{S}_\infty$. All the other cases can be similarly proved. The cross-correlation function between two sequences in $\mathcal{S}_\infty$, $m(2t)+m(2d(t+j))$ and $m(2t)+m(2d(t+k))$, is given as

$$
\begin{aligned}
C(\tau) &= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)})+\mathrm{tr}_1^n(\alpha^{2d(t+\tau+j)})-\mathrm{tr}_1^n(\alpha^{2t})-\mathrm{tr}_1^n(\alpha^{2d(t+k)})} \\
&= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2t}(\alpha^{2\tau}-1))+\mathrm{tr}_1^n(\alpha^{2dt}(\alpha^{2d(\tau+j)}-\alpha^{2dk}))}. \qquad (3.1)
\end{aligned}
$$

Let $a = \alpha^{2\tau} - 1$ and $b' = \alpha^{2d(\tau+j)} - \alpha^{2dk}$. Then (3.1) can be written as

$$C(\tau) = \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(a\alpha^{2t}+b'\alpha^{2dt})}.$$

Here, note that

$$\begin{aligned}2dt &= 2(N - p^{n-1})t \\ &= 2(\frac{p^n - 1}{2} - p^{n-1})t \\ &= (p^n - 1 - 2p^{n-1})t \\ &= -2p^{n-1}t \\ &= -2p^{-1}t \text{ (mod } p^n - 1).\end{aligned}$$

Since $2dt = -2p^{-1}t$ (mod $p^n - 1$), we have

$$\begin{aligned}\mathrm{tr}_1^n(b'\alpha^{2dt}) &= \mathrm{tr}_1^n(b'\alpha^{-2p^{-1}t}) \\ &= \mathrm{tr}_1^n((b'\alpha^{-2p^{-1}t})^p) \\ &= \mathrm{tr}_1^n(b'^p\alpha^{-2t}).\end{aligned}$$

Let $b = b'^p$. Then we have

$$\begin{aligned}C(\tau) &= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(a\alpha^{2t}+b\alpha^{-2t})} \\ &= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(a(\alpha^t)^2+b(\alpha^t)^{-2})} \\ &= \sum_{y\in QR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})}. \qquad (3.2)\end{aligned}$$

In order to compute $C(\tau)$ in (3.2), we can use the Kloosterman sum and the generalized Kloosterman sum given as

$$\begin{aligned}K(\chi_1; a, b) &= \sum_{y\in\mathbb{F}_{p^n}^*} \omega^{\mathrm{tr}_1^n(ay+by^{-1})} \\ &= \sum_{y\in QR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})} + \sum_{y\in QNR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})}\end{aligned}$$

$$L(\chi_1; a, b) = \sum_{y\in\mathbb{F}_{p^n}^*} \eta(y)\omega^{\mathrm{tr}_1^n(ay+by^{-1})}$$

$$= \sum_{y \in QR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})} - \sum_{y \in QNR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})}.$$

From Lemma 3.13, we have an upper bound on $L(\chi_1; a, b)$, namely $|L(\chi_1; a, b)| \leq 2\sqrt{p^n}$.

Since p is an odd prime which is 3 mod 4 and n is an odd integer, -1 is nonsquare. Therefore, as y runs through QR, $-y$ does through QNR and we have

$$\overline{\sum_{y \in QR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})}} = \sum_{y \in QNR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})}.$$

Now we are ready to show that the absolute value of cross-correlation $C(\tau)$ is upper bounded by $2\sqrt{N + \frac{1}{2}} = \sqrt{2p^n}$.

From the previous argument, we can set

$$\sum_{y \in QR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})} = u + v\sqrt{-1}$$

and

$$\sum_{y \in QNR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})} = u - v\sqrt{-1}$$

where u, v are real numbers.

From the definitions of the Kloosterman and the generalized Kloosterman sums, we obtain

$$K(\chi_1; a, b) = 2u \tag{3.3}$$

$$L(\chi_1; a, b) = 2v\sqrt{-1}. \tag{3.4}$$

For cross-correlation and nontrivial autocorrelation, it can be easily shown that $a \neq 0$ or $b \neq 0$. If $a = 0$, then by definition of a, $\alpha^{2\tau} = 1$, which implies $\tau = N = 0 \pmod{N}$. Also note that

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

$$\begin{aligned}
&= \frac{p^{n+1}-p}{2} - 1 \\
&= \frac{(p-1)p^n + p^n - p}{2} - 1 \\
&= \frac{p-1}{2}p^n + \frac{p^n - p}{2} - 1 \\
&= \frac{p-1+p^n-p}{2} - 1 \\
&= \frac{p^n-1}{2} - 1 \\
&= -1 \pmod{p^n - 1}.
\end{aligned}$$

Therefore we have

$$\begin{aligned}
b &= \alpha^{2d(\tau+j)p} - \alpha^{2dkp} \\
&= \alpha^{-2(\tau+j)} - \alpha^{-2k} \\
&= \frac{\alpha^{-2j}}{a+1} - \alpha^{-2k}.
\end{aligned}$$

It is easy to check that $a = b = 0$ corresponds to the in-phase autocorrelation. Therefore, from Lemma 3.8, we have $|K(\chi_1; a, b)| \leq 2\sqrt{p^n}$.

Thus from Lemmas 3.8 and 3.13 and (3.3) and (3.4), we have

$$\begin{aligned}
|u| &\leq \sqrt{p^n} \\
|v| &\leq \sqrt{p^n}.
\end{aligned}$$

Finally, we obtain

$$\begin{aligned}
|R(\tau)| &= \Big|\sum_{y \in QR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})}\Big| \\
&= |u + vi| \\
&\leq \sqrt{2p^n} \\
&= 2\sqrt{N + \frac{1}{2}}.
\end{aligned}$$

The proof for cross-correlation bound in each of the other cases is quite similar, because the cross-correlation expression eventually becomes the

Table 3.1: Values of a and b for each case.

Sequence set 1	Sequence set 2	a	b
$\mathcal{S}_1$	$\mathcal{S}_1$	$\alpha^{2\tau} - 1$	$(\alpha^{2d(\tau+j)} - \alpha^{2dk})^p$
$\mathcal{S}_1$	$\mathcal{S}_2$	$\alpha^{2\tau} - \alpha$	$(\alpha^{2d(\tau+j)} - \alpha^{2dk})^p$
$\mathcal{S}_1$	$\mathcal{S}_3$	$\alpha^{2\tau} - 1$	$(\alpha^{2d(\tau+j)} - \alpha^{2dk+1})^p$
$\mathcal{S}_1$	$\mathcal{S}_4$	$\alpha^{2\tau} - \alpha$	$(\alpha^{2d(\tau+j)} - \alpha^{2dk+1})^p$
$\mathcal{S}_2$	$\mathcal{S}_2$	$\alpha^{2\tau+1} - \alpha$	$(\alpha^{2d(\tau+j)} - \alpha^{2dk})^p$
$\mathcal{S}_2$	$\mathcal{S}_3$	$\alpha^{2\tau+1} - 1$	$(\alpha^{2d(\tau+j)} - \alpha^{2dk+1})^p$
$\mathcal{S}_2$	$\mathcal{S}_4$	$\alpha^{2\tau+1} - \alpha$	$(\alpha^{2d(\tau+j)} - \alpha^{2dk+1})^p$
$\mathcal{S}_3$	$\mathcal{S}_3$	$\alpha^{2\tau} - 1$	$(\alpha^{2d(\tau+j)+1} - \alpha^{2dk+1})^p$
$\mathcal{S}_3$	$\mathcal{S}_4$	$\alpha^{2\tau} - \alpha$	$(\alpha^{2d(\tau+j)+1} - \alpha^{2dk+1})^p$
$\mathcal{S}_4$	$\mathcal{S}_4$	$\alpha^{2\tau+1} - \alpha$	$(\alpha^{2d(\tau+j)+1} - \alpha^{2dk+1})^p$

Kloosterman sum over the quadratic residue as in (3.2) using the same technique. The only differences are values of constants a and b in (3.1). We summarize values of a and b for each case in Table 3.1.

Thus the proof is complete. □

3.7. Size of Sequence Family

The family size of $\mathcal{S}$ is $2(p^n - 1)$, which is four times larger than the period. In the following theorem, we can show that any two sequences in S are cyclically inequivalent.

Theorem 3.15. The family size of $\mathcal{S}$ is $2(p^n - 1)$. More precisely, there are no cyclically equivalent sequences in S.

Proof. Suppose that there are two sequences $v(t)$ and $w(t)$ in $\mathcal{S}$ which are cyclically equivalent each other. Let $C(\tau)$ be a cross-correlation between $v(t)$ and $w(t)$. Then there exists τ_0 such that $0 \leq \tau_0 < N$ and $C(\tau_0) = N$. Recall that any cross-correlation values of sequences in $\mathcal{S}$ can be written as a Kloosterman sum over the quadratic residue. Let

$$C(\tau_0) = \sum_{y \in QR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})} = u + vi$$

$$\sum_{y \in QNR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})} = u - vi.$$

Since $C(\tau_0) = N$, we have $v = 0$. Therefore $u = N$. Thus

$$K(\chi; a, b) = 2u = 2N \Longrightarrow K(\chi; a, b) = p^n - 1.$$

It is known that if $K(\chi; a, b) = p^n - 1$, then $a, b = 0$. Therefore it suffices to show that $a, b = 0$ implies $v(t) = w(t)$. It is already discussed that $a, b = 0$ implies $v(t) = w(t)$ when $v(t), w(t) \in \mathcal{S}_\infty$. The proofs for the case of $\mathcal{S}_\in, \mathcal{S}_\ni, \mathcal{S}_\triangle$ are similar. It is also easily verified that if $v(t) \in \mathcal{S}_\|$ and $w(t) \in \mathcal{S}_\updownarrow$ for $k \neq l$, then $a \neq 0$ or $b \neq 0$. For example, let $l = 1$, $k = 2$. Then

$$\begin{aligned}
&C_{i,j}(\tau_0) \\
&= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau_0)}) + \mathrm{tr}_1^n(\alpha^{2d(t+\tau_0+i)}) - \mathrm{tr}_1^n(\alpha^{2t+1}) - \mathrm{tr}_1^n(\alpha^{2d(t+j)})} \\
&= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2t}(\alpha^{2\tau_0} - \alpha)) + \mathrm{tr}_1^n(\alpha^{2dt}(\alpha^{2d\tau_0+2di} - \alpha^{2dj}))} \\
&= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2t}(\alpha^{2\tau_0} - \alpha)) + \mathrm{tr}_1^n(\alpha^{2dpt}(\alpha^{2dp\tau_0+2dpi} - \alpha^{2dpj}))} \\
&= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2t}(\alpha^{2\tau_0} - \alpha)) + \mathrm{tr}_1^n(\alpha^{-2t}(\alpha^{-2\tau_0-2i} - \alpha^{-2j}))} \\
&= \sum_{y \in QR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})}
\end{aligned}$$

where $a = \alpha^{2\tau_0} - \alpha$ and $b = \alpha^{-2\tau_0-2i} - \alpha^{-2j}$. Since $\alpha^{2\tau_0} \in QR$ and $\alpha \in QNR$, we can conclude that $a \neq 0$. The proofs for the other cases are similar. □

The new family is not optimal with respect to the Welch bound, which is rather insensitive to the family size. In fact, the upper bound on the correlation magnitudes of the proposed sequence family is approximately twice the Welch's lower bound, but its family size is four times the period of the sequences. On the other hand, the Sidel'nikov lower bound [23] on the maximum correlation magnitude depends not only on the period but also on the family size. Here, we are going to measure how close the proposed sequence family is to the optimality with respect to the Sidel'nikov's bound given below.

Lemma 3.16 (Sidel'nikov [6])**.** Let $\mathcal{S}$ be a family of M p-ary sequences of period N, where p is an odd prime. Let C_{max} be the maximum magnitude of correlation values. Then

$$C_{max}^2 > \frac{k+1}{2}(2N-k) - \frac{2^k N^{2k+1}}{M(k!)^2\binom{2N}{k}}$$

for all $k \geq 0$. □

Here, let $k = 1$ and $M = 4N$. Then we have

$$C_{max}^2 > 2N - 1 - \frac{2N^3}{4N2N} = 2N - 1 - \frac{1}{4}N = \frac{7}{4}N - 1.$$

Thus

$$C_{max} > \sqrt{\frac{7}{4}N - 1} \approx 1.3228\sqrt{N}.$$

Therefore we can see that the maximum magnitude of the nontrivial correlation values of the proposed family is approximately $0.7\sqrt{N}$ larger than the Sidel'nikov's bound. Table 3.2 shows the parameters of some well known sequence families and the new family derived in this chapter.

3.8. An Example

For $p = 3$, $n = 3$, we have $N = 13$ and $d = 4$. Let α be a primitive element of $\mathbb{F}_{3^3}$ with a minimal polynomial $x^3 + 2x + 1$. Then the sequence family is given as:

$$\begin{aligned}
\mathcal{S}_\infty = \{&(0020022220020), (1201121211021), (0012111121002),\\
&(1122010221111), (2221001222202), (0211211200110),\\
&(0110011012221), (2101012100001), (2011020011100),\\
&(1111102122120), (2112220202022), (2120101001010),\\
&(2202212021220)\}\\
\mathcal{S}_\in = \{&(0110220002100), (1021022020101), (0102012200112),\\
&(1212211000221), (2011202001012), (0001112012220),\\
&(0200212121001), (2221210212111), (2101221120210),\\
&(1201000201200), (2202121011102), (2210002110120),\\
&(2022110100000)\}\\
\mathcal{S}_\ni = \{&(0200000101122), (0001200022011), (1010202201201),\\
&(1100221020102), (2000112212112), (1002021102210),\\
&(1021110000222), (1212002010012), (0121222111212),\\
&(2210120120211), (0102100210200), (2022201110121),\\
&(1220210112000)\}
\end{aligned}$$

$$\begin{aligned}\mathcal{S}_{\triangle} = \{&(0020201210202), (0121101101121), (1100100010011),\\ &(1220122102212), (2120010021222), (1122222211020),\\ &(1111011112002), (1002200122122), (0211120220022),\\ &(2000021202021), (0222001022010), (2112102222201),\\ &(1010111221110)\}\end{aligned}$$

In general, the number of correlation values or the correlation distribution is irregular. For instance, the cross-correlation distribution between $a(t) = (1201121211021)$ and $b(t) = (0102012200112)$ is given as:

$$C_{a,b}(\tau) = \begin{cases} -3.5 + 2.59808\sqrt{-1} & \text{once} \\ -3.5 - 2.59808\sqrt{-1} & \text{once} \\ -0.5 - 2.59808\sqrt{-1} & \text{once} \\ 1 & \text{3 times} \\ 4 & \text{2 times} \\ -5 & \text{once} \\ 4 + 5.19615\sqrt{-1} & \text{once} \\ -2 + 5.19615\sqrt{-1} & \text{once} \\ -2 - 5.19615\sqrt{-1} & \text{once} \\ -2 & \text{once.} \end{cases}$$

But for $c(t) = (0001200022011)$ and $d(t) = (1100100010011)$, the cross-correlation is

$$C_{c,d}(\tau) = \begin{cases} 2.5 - 2.59808\sqrt{-1} & \text{2 times} \\ -0.5 + 2.59808\sqrt{-1} & \text{3 times} \\ -0.5 - 2.59808\sqrt{-1} & \text{2 times} \\ 4 + 5.19615\sqrt{-1} & \text{2 times} \\ -2 & \text{2 times} \\ 1 & \text{2 times.} \end{cases}$$

Note that the number of cross-correlation values and the correlation distribution are different.

3.9. Related Work

After [57] and [58] are published, a generalization of the sequence family is given. Kim, Chae, and Song [61] proposed the generalization method by extending the alphabet and the decimation parameters. Specifically, for an integer e satisfying $e|p^n - 1$, they proposed a family of e^2N p-ary sequences, each sequence in $\mathcal{S}$ has period N, and the magnitudes of correlations of sequences in $\mathcal{S}$ are upper bounded by $2\sqrt{p^n} = 2\sqrt{eN+1}$ [61].

Definition 3.17 (Kim, Chae, and Song [61])**.** Let p be a prime and n be a positive integer. Let $m(t)$ be a p-ary m-sequence of period $p^n - 1$. Let $N = \frac{p^n-1}{e}$, where e is a positive divisor of $p^n - 1$ and $d = N - p^{n-1}$. Since $\gcd(d, N) = 1$, the decimated sequences $m(et)$ and $m(edt)$ have the period $N = (p^n - 1)/e$. Define the family $\mathcal{S}$ of sequences of period N to be

$$\mathcal{S} = \{s_{k,i,u}(t) | 0 \leq t < N\} \tag{3.5}$$

where $k = 0, 1, ..., e-1$, $u = 0, 1, ..., e-1$, $i = 0, 1, ..., N-1$, and

$$s_{k,i,u}(t) = m(et + k) + m(ed(t + i) + u).$$

□

The following theorem shows that the family consists of sequences which are cyclically inequivalent.

Theorem 3.18 (Kim, Chae, and Song [61]). Let $\mathcal{S}$ be the family of sequences defined in (3.5). Then, the magnitude of nontrivial autocorrelation and cross-correlation of sequences in $\mathcal{S}$ is upper bounded by $2\sqrt{p^n}$ and no two sequences in $\mathcal{S}$ are cyclically equivalent and thus, $|\mathcal{S}| = e^2 N$, provided that

$$e < \frac{\sqrt{p^n} - 1/\sqrt{p^n}}{2}.$$

□

Note that by appropriately choosing e, we can utilize the tradeoff between the family size $e^2 N$ and the period $\frac{p^n-1}{2}$.

3.10. Conclusion

In this chapter, a new family of p-ary sequences with low correlation is constructed. The sequence family can be constructed in $\mathbb{F}_{p^n}$, with a prime p of 3 mod 4 and an odd integer n. The period of sequences is $\frac{p^n-1}{2}$. Sequences in the family are obtained using shifts and additions of decimated m-sequences $m(2t)$ and $m(2dt)$ with the decimation factor $d = N - p^{n-1}$. The upper bound on the magnitude of nontrivial correlation values of the sequence family can be deduced by the Kloosterman sums, which is asymptotically two times the Welch's lower bound and approximately 1.5 times the Sidel'nikov's lower bound. The size of the sequence family is $2(p^n - 1)$, 4 times the period of the sequences. Some example of the family is given and the generalization of Kim, Chae, and Song [61] is discussed.

Table 3.2: Comparison of well-known families of sequences.

Family	Alphabet	Period N	R_{max}	Family size
Gold, odd n [4]	2	$2^n - 1$	$1 + \sqrt{2(N+1)}$	$N + 2$
Gold, even n [4]	2	$2^n - 1$	$1 + 2\sqrt{N+1}$	$N + 2$
Kasami [2] [3]	2	$2^n - 1$	$1 + \sqrt{N+1}$	$\sqrt{N}$
Trachtenberg [7]	odd p	$p^n - 1$	$1 + \sqrt{(N+1)p}$	$N + 2$
Helleseth [11]	odd p	$p^n - 1$	$1 + 2\sqrt{N+1}$	$N + 2$
KM [23]	odd p	$p^n - 1$	$1 + \sqrt{N+1}$	$N + 1$
LK [24]	odd p	$p^n - 1$	$1 + \sqrt{N}$	$\sqrt{N}$
$\mathcal{V}^{(c_1)}$ [39]	$M > 2$ even	$p^n - 1$ (odd p)	$2\sqrt{N+1} + 2$	$N + M - 1$
$\mathcal{V}$ [39]	M	$p^n - 1$ (odd p)	$3\sqrt{N+1} + 1$	$(\frac{N}{2} + 1)(M - 1)$
$\tilde{\mathcal{U}}$ [39]	M even	$p^n - 1$ (odd p)	$2\sqrt{N+1} + 6$	$(N + 1)\frac{M}{2} - 1$
$\mathcal{U}$ [39]	M	$p^n - 1$ (odd p)	$3\sqrt{N+1} + 5$	$\frac{M(M-1)(N-1)}{2} + M - 1$
Ω_r [44] $(0 \leq r \leq p-2)$	p	p	$(r + 1)\sqrt{N} + 2$	$(N - 2)N^r$
$\mathcal{L}$ $(p = 2)$ [31]	M	$2^n - 1$	$3\sqrt{N+1} + 5$	$(M - 1)^2(\frac{N-1}{2}) + M - 1$
$\mathcal{L}$ (odd p) [31]	M	$p^n - 1$	$3\sqrt{N+1} + 5$	$(M - 1)^2(\frac{N}{2} - 1)$ $+ \frac{M(M-1)}{2}$
$\mathcal{F}_{\mathbf{r}}^{(a)}$ [38]	M	p	$2\sqrt{N} + 5$	$\frac{N-1}{2} + M - 1$
$\mathcal{F}_{\mathbf{r}}$ [38]	M	p	$3\sqrt{N} + 4$	$\frac{(M-1)^2(N-1)}{2} + M - 1$
$\tilde{\mathcal{F}}_{\mathbf{s}}$ [38]	M	$p^n - 1$	$2\sqrt{N+1} + 6$	$\frac{(M-1)}{2}N + \lfloor \frac{M-1}{2} \rfloor$
$\mathcal{G}_{\mathbf{r}}^{(\delta,2)}$ [39] $(\delta \neq 0)$	M	p	$4\sqrt{N} + 7$	$(M - 1)$ $+(\frac{N-1}{2})(M - 1)^2$ $+ \frac{(N-1)(N-3)}{8}(M^2 - 3M + 3)$
$\mathcal{H}_{\mathbf{r}}^{(2)}$ [39]	M	p	$5\sqrt{N} + 6$	$(M - 1)$ $+(\frac{N-1}{2})(M - 1)^2$ $+ \frac{(N-1)(N-3)}{8}(M - 1)^3$
$\mathcal{G}_{\mathbf{s}}^{(\delta,2)}$ [39] $(\delta \neq 0)$	M	$p^n - 1$	$4\sqrt{N+1} + 8$	$(M - 1)$ $+(\frac{N-2}{2})(M - 1)^2$ $+ \frac{(N-2)(N-4)}{8}(M^2 - 3M + 3)$
$\mathcal{H}_{\mathbf{s}}^{(2)}$ [39]	M	$p^n - 1$	$5\sqrt{N+1} + 7$	$(M - 1)$ $+(\frac{N-2}{2})(M - 1)^2$ $+ \frac{(N-2)(N-4)}{8}(M - 1)^3$
New	p (3 mod 4)	$\frac{p^n-1}{2}$	$2\sqrt{N + \frac{1}{2}}$	$4N$

Chapter 4. On the Cross-Correlation between Two Decimated p-ary m-Sequences by 2 and $4p^{n/2} - 2$

Based on the work by Helleseth [71], for an odd prime p and an even integer $n = 2m$, the cross-correlation values between two decimated m-sequences by the decimation factors 2 and $4p^{n/2} - 2$ are derived. Their cross-correlation function is at most 4-valued, that is, $\frac{-1 \pm p^{n/2}}{2}$, $\frac{-1+3p^{n/2}}{2}$, and $\frac{-1+5p^{n/2}}{2}$. From this result, for $p^m \neq 2 \mod 3$, a new sequence family with family size $4N$ and the maximum correlation magnitude upper bounded by $\frac{-1+5p^{n/2}}{2} \simeq \frac{5}{\sqrt{2}}\sqrt{N}$ is constructed, where $N = \frac{p^n-1}{2}$ is the period of sequences in the family. [1]

4.1. Introduction

Pseudonoise sequences have wide applications in various areas, including signal processing, channel estimation, radar, cryptography, and communications. In particular, for code-division multiple access communication systems, each user in the cell is assigned a user signature sequence and correlation values between sequences should be low for multiplexing

[1] The material of this chapter is primarily based on the following paper: Copyright ©2015 IEICE from Ji-Youp Kim, Chang-Min Cho, Wi-Jik Lee and Jong-Seon No, "On the Cross-Correlation between Two Decimated p-Ary m-Sequences by 2 and $4p^{n/2} - 2$," to apper in *IEICE Transactions on Communications*, vol. E98-B, no. 3, Mar. 2015.

message signals. Low autocorrelation of each sequence is important for synchronization and low cross-correlation between sequences are crucial for intra-cell interference mitigation. Therefore, many studies have constructed sequence families with low auto- and cross-correlations. Also, since large family size implies that a large number of users can communicate with each other in one cell, sequence families with low correlation and large family size are preferred.

One of the popular methods to construct sequence families is to investigate the correlation property of decimated m-sequences. If m-sequence $m(t)$ and decimated sequence $m(dt)$ by the decimation factor d have low cross-correlation, then by using shift-and-add method, a sequence family with good correlation property can be constructed easily. Thus, many researchers have attempted to find "good" decimation values and to investigate the correlation values of the decimated sequences. Helleseth [71] studied various decimation values for binary and nonbinary m-sequences. For an odd prime p, $n = 4k$, Seo, Kim, No, and Shin [37] derived the exact correlation distribution between m-sequences and their $\frac{p^{2k}+1}{2}$ decimated sequences by $d = (\frac{p^{2k}+1}{2})^2$. Luo [42] extended the result of [37] to the case $n = 2m$ and $p^m = 1 \mod 4$. Muller [27] employed the quadratic form technique to derive an upper bound on the cross-correlation between the ternary m-sequence and its decimated sequence by $d = \frac{3^n+1}{3+1} + \frac{3^n-1}{2}$. Hu, Li, Mills, Muller, Sun, Willems, Yang, and Zhang [28] generalized this result to the case $p = 3 \mod 4$. Xia, Zeng, and Hu [46] calculated the exact distribution of correlation values. Later, Choi, Kim, and No [55] extended

Xia's result to the more general decimation factor $d = \frac{p^n+1}{p^k+1} + \frac{p^n-1}{2}$. Seo, Kim, No, and Shin [36] derived the cross-correlation distribution between p-ary m-sequences and decimated sequences by $d = p^k + 1$ with even n and $\gcd(n, k) = 1$. Choi, Lim, No, and Chung [52] investigated an upper bound on the correlation magnitude for $d = \frac{(p^m+1)^2}{2(p+1)}$ and $n = 2m$, where m is an odd integer. Luo, Helleseth, and Kholosha [43] extended the result for $p = 3 \mod 4$ case to the decimation $d = \frac{(p^m+1)^2}{2(p^k+1)}$ with odd m and $k|m$, and derived the correlation distribution. Sun, Wang, Li, and Yan [56] derived the exact distribution of the cross-correlation for $p = 1 \mod 4$ and $d = \frac{(p^m+1)^2}{2(p^k+1)}$ when m is odd and $k|m$. Xia and Chen [48] determined the distribution of the cross-correlation values for more general case $d = \frac{(p^m+1)^2}{2(p^k+1)}$, where p is any odd prime and m is any integer with odd m/k. Kim, Choi, Lim, No, and Chung [59] studied the cross-correlation between ternary m-sequences and their decimated sequences by $d = \frac{3^{4k+2}-3^{2k+1}+2}{4} + 3^{2k+1}$, where $n = 4k + 2$ and obtained the upper bound. Later, Xia, Chen, Helleseth, and Li [49] generalized the result to the arbitrary odd prime p and $d = \frac{(p^m+1)(p^m+p-1)}{(p+1)}$ and derived the correlation values. Some recent results on the cross-correlation between m-sequences and their decimated sequences are summarized in Table 4.1. For more detail, the reader is referred to [54].

Recently, there have been some results for "half-period" ($N = \frac{p^n-1}{2}$) sequence family construction. Using decimation $d = \frac{p^n-1}{2} - p^{n-1}$, Kim, Choi, and No [58] constructed a p-ary sequence family of period $\frac{p^n-1}{2}$, where $p = 3 \mod 4$ and n is an odd integer. Kim, Chae, and Song [61]

Table 4.1: Previous works on the cross-correlation between p-ary m-sequences and their decimated sequences.

	Alphabet	n	d	$\mathcal{N}$	$C_{\max}$
Helleseth [11]	odd p	even n, $p^{n/2} \neq 2 \mod 3$	$2p^{n/2} - 1$	4	$-1 + 2p^{n/2}$
Seo *et al.* [37]	odd p	$4k$	$(\frac{p^{2k}+1}{2})^2$	4	$-1 + 2p^{n/2}$
Luo [42]	$p^m = 1 \mod 4$	$n = 2m$	$(\frac{p^{m}+1}{2})^2$	4	$-1 + 2p^{n/2}$
Muller [27]	$p = 3$	odd	$\frac{3^n+1}{3+1} + \frac{3^n-1}{2}$	$\star$	$1 + 2\sqrt{p^n}$
Hu *et al.* [28]	$p = 3 \mod 4$	odd	$\frac{p^n+1}{p+1} + \frac{p^n-1}{2}$	$\star$	$1 + \frac{p+1}{2}\sqrt{p^n}$
Xia *et al.* [46]	$p = 3 \mod 4$	odd	$\frac{p^n+1}{p+1} + \frac{p^n-1}{2}$	9	$-1 - p^{n/2}\frac{\sqrt{-1}(p+1)}{2}$
Choi *et al.* [55]	$p = 3 \mod 4$	odd n, $k\|n$	$\frac{p^n+1}{p^k+1} + \frac{p^n-1}{2}$	9	$-1 - j\frac{p^k+1}{2}p^{n/2}$
Seo *et al.* [36]	odd p	even n, $\gcd(n, k) = 1$	$p^k + 1$	9	$\simeq p\sqrt{p^n} + 1$
Choi *et al.* [52]	odd p	$n = 2m$, m odd	$\frac{(p^m+1)^2}{2(p+1)}$	$\star$	$1 + \frac{p+1}{2}p^{n/2}$
Luo *et al.* [43]	$p = 3 \mod 4$	$n = 2m$, m odd, $k\|m$	$\frac{(p^m+1)^2}{2(p^k+1)}$	6	$\frac{1}{2}(-1 - p^k)p^m - 1$
Sun *et al.* [56]	$p = 1 \mod 4$	$n = 2m$, m odd, $k\|m$	$\frac{(p^m+1)^2}{2(p^k+1)}$	6	$\frac{1}{2}(1 - p^k)p^m - 1$
Xia and Chen [48]	odd p	$n = 2m$, $k\|m$, m/k odd	$\frac{(p^m+1)^2}{2(p^k+1)}$	6	$\frac{1}{2}(-1 - p^k)p^m - 1$
Kim *et al.* [59]	$p = 3$	$n = 4k + 2$	$\frac{3^{4k+2}-3^{2k+1}+2}{4} + 3^{2k+1}$	$\star$	$4.5\sqrt{p^n} + 1$
Xia *et al.* [49]	odd p	$n = 2m$, odd m	$\frac{(p^m+1)(p^m+p-1)}{(p+1)}$	$2p + 1$	$-1 - p^{m+1}$

$\star$ denotes that the authors derive only the upper bound on the magnitude of the correlation.

$\mathcal{N}$ is the number of correlation values and $C_{\max}$ is the maximum magnitude of the correlation. ©2015 IEICE.

generalized this result to the arbitrary odd prime p and any integer n, where the period is $\frac{p^n-1}{e}$ with $e|p^n-1$ and $e < \frac{\sqrt{p^n}-1/\sqrt{p^n}}{2}$. For $d = p^m+1$, Xia and Chen [47] constructed a half-period sequence family and derived its correlation distribution. Lee, Kim, and No [62] constructed p-ary sequence families of period $\frac{p^n-1}{2}$ with low correlation for $d=4$ and $\frac{p^n+1}{2}$. Lately, Cho, Kim, and No [64], based on the previous works by Seo, Kim, No, and Shin [37] and Luo [42], studied the cross-correlation between two decimated m-sequences by 2 and $\frac{(p^m+1)^2}{2}$. In Table 4.2, we list these works for comparison.

In this chapter, based on the Helleseth's work [71], for an odd prime p and an even integer $n=2m$, the cross-correlation values between two decimated m-sequences by 2 and $d' = 4p^{n/2}-2$ are derived. The cross-correlation is at most 4-valued and takes the values of $\frac{-1\pm p^{n/2}}{2}$, $\frac{-1+3p^{n/2}}{2}$, and $\frac{-1+5p^{n/2}}{2}$. Using this result, for $p^m \neq 2 \mod 3$, a new sequence family with family size $4N$ and the maximum correlation magnitude upper bounded by $\frac{-1+5p^{n/2}}{2} \simeq \frac{5}{\sqrt{2}}\sqrt{N}$ is constructed, where $N = \frac{p^n-1}{2}$ is the period of sequences in the family.

This chapter is organized as follows. In Section 4.2, we introduce half-period sequence families, previous works, and preliminaries. Next, in Section 4.3, we derive the values of the cross-correlation between p-ary m-sequences and decimated sequences by 2 and $4p^{n/2}-2$. In Section 4.4, we give examples of actual correlation values. Then we propose the construction of the half-period sequence families and derive the correlation values in Section 4.5. In Section 4.6, we discuss about the distribution of the correlation. Lastly, we conclude this chapter in Section 4.7.

4.2. Decimated Sequences of Period $\frac{p^n-1}{2}$

Let $m(t)$ be a p-ary m-sequence of period p^n-1 and d be a decimation factor. Consider two decimated sequences $m(2t+i)$ and $m(2dt+j)$, where $0 \leq i, j \leq 1$. Note that we decimate $m(dt)$ further by 2 as $m(2dt)$. The period of $m(2t+i)$ is $N = \frac{p^n-1}{2}$. Then the cross-correlation $C_{i,j}(\tau)$ between $m(2t+i)$ and $m(2dt+j)$ is given as

$$\begin{aligned} C_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{m(2(t+\tau)+i)-m(2dt+j)} \\ &= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i}-\alpha^{2dt+j})}. \end{aligned} \tag{4.1}$$

Since gcd$(2d$, $p^n-1)$ is a multiple of 2, we have

$$\sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i}-\alpha^{2dt+j})} = \sum_{t=N}^{p^n-2} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i}-\alpha^{2dt+j})}.$$

Therefore, (4.1) can be rewritten as

$$\begin{aligned} C_{i,j}(\tau) &= \frac{1}{2} \sum_{t=0}^{p^n-2} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i}-\alpha^{2dt+j})} \\ &= \frac{1}{2} \sum_{x \in \mathbb{F}_{p^n}^*} \omega^{\mathrm{tr}_1^n(ax^2-bx^{2d})} \end{aligned}$$

where $x = \alpha^t$, $a = \alpha^{2\tau+i}$, and $b = \alpha^j$.

In Chapter 3, for an odd prime $p = 3 \mod 4$ and an integer n, families of p-ary sequences of period $\frac{p^n-1}{2}$ with low correlation and family size $2(p^n-1)$ were introduced. Later, Xia and Chen [47] proposed families

Table 4.2: Some known sequence families of period $\frac{p^n-1}{2}$.

Family	Alphabet	n	Period N	Family size	$C_{\max}$
Kim *et al.* [57]	$p = 3 \mod 4$	odd	$\frac{p^n-1}{2}$	$4N$	$2\sqrt{N+\frac{1}{2}}$
Kim *et al.* [61]	odd p	even or odd	$\frac{p^n-1}{e}$	e^2N	$2\sqrt{eN+1}$
Xia and Chen [47]	$p \equiv 1 \pmod 4$	even or odd	$\frac{p^n-1}{2}$	$4N$	$\frac{p}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}$
	$p \equiv 3 \pmod 4$	even	$\frac{p^n-1}{2}$	$4N$	$\frac{p}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}$
Lee *et al.* [62]	$p = 3 \mod 4$	odd	$\frac{p^n-1}{2}$	$4N$	$\simeq \frac{3}{\sqrt{2}}\sqrt{N}$
Cho *et al.* [64]	odd p	even	$\frac{p^n-1}{2}$	$2\sqrt{2N+1}$	$\simeq \frac{3}{\sqrt{2}}\sqrt{N}$
New	odd p	$n = 2m$ with $p^m \neq 2 \mod 3$	$\frac{p^n-1}{2}$	$4N$	$\simeq \frac{5}{\sqrt{2}}\sqrt{N}$

of p-ary half-period sequences for more general p. We introduce these as previous works for half-period sequence constructions.

Theorem 4.1 (in Chapter 3)**.** Let $p = 3 \mod 4$ be an odd prime and n be an odd integer. Let $N = \frac{p^n-1}{2}$ and $d = N - p^{n-1}$. Let α be a primitive element of $\mathbb{F}_{p^n}$. Then the sequence family is defined as

$$S = \{\mathrm{tr}_1^n(\alpha^{2t+i}) + \mathrm{tr}_1^n(\alpha^{2d(t+k)+j}) | 0 \le i, j \le 1, 0 \le k < N\}.$$

Then the maximum magnitude of the correlation between sequences in S is upper bounded by $2\sqrt{N + \frac{1}{2}}$ and the family size is $4N = 2(p^n - 1)$. □

Theorem 4.2 (Xia and Chen [47])**.** Let p be an odd prime and m, n be positive integers. Suppose $e = \gcd(m, n)$ and $\frac{n}{e} \ge 3$. Let $N = \frac{p^n-1}{2}$, $d = p^m + 1$, and α be a primitive element of $\mathbb{F}_{p^n}$. Then the sequence family is defined as

$$S = \{\mathrm{tr}_1^n(\alpha^{2t+i}) + \mathrm{tr}_1^n(\alpha^{d(t+k)+j}) | 0 \le i, j \le 1, 0 \le k < N\}.$$

Then the maximum magnitude of the correlation between sequences in S is

$$\begin{cases} \frac{1}{2}(p^e\sqrt{p^n} + 1), & \text{if } \eta(-1) = 1 \\ \frac{1}{2}(p^e\sqrt{p^n + \frac{1}{p^{2e}}}), & \text{if } \eta(-1) = -1 \end{cases}$$

and the family size is $4N = 2(p^n - 1)$, where η is a quadratic character defined on $\mathbb{F}_{p^n}$. □

Recently, Cho, Kim, and No [64] derived the distribution of cross-correlation values of the above form for $2d = 2(\frac{p^m+1}{2})^2$, $n = 2m$, and $p^m = 1 \mod 4$, where the original decimation factor $d = (\frac{p^m+1}{2})^2$ was first studied by Seo, Kim, No and Shin [37] and later by Luo [42].

Theorem 4.3 (Cho, Kim, and No [63] [64])**.** Let p be an odd prime and $n = 2m$ with $p^m = 1 \mod 4$. Let $d = (\frac{p^m+1}{2})^2$. Then the cross-correlation distribution between $\mathrm{tr}_1^n(\alpha^{2t+i})$ and $\mathrm{tr}_1^n(\alpha^{2dt})$, $i \in \{0, 1\}$, is

given as follows.
(i) For $i = 0$

$$C(\tau) = \begin{cases} \frac{-1-p^m}{2}, & \frac{1}{8}(3p^n - 4p^m - 7) \text{ times} \\ \frac{-1+p^m}{2}, & \frac{p^m+1}{2} \text{ times} \\ \frac{-1+3p^m}{2}, & \frac{1}{8}(p^n - 1) \text{ times.} \end{cases}$$

(ii) For $i = 1$

$$C(\tau) = \begin{cases} \frac{-1-p^m}{2}, & \frac{1}{4}(p^n - 1) \text{ times} \\ \frac{-1+p^m}{2}, & \frac{1}{4}(p^n - 1) \text{ times.} \end{cases}$$

□

Lee, Kim, and No [62], using Weil bound, constructed two families of p-ary sequences of period $\frac{p^n-1}{2}$ with low correlation. The decimations are $d = 4$ and $d = \frac{p^n+1}{2}$.

Theorem 4.4 (Lee, Kim, and No [62])**.** Let p be an odd prime and n be an odd integer. Let $N = \frac{p^n-1}{2}$ and $d = 4$ or $d = \frac{p^n+1}{2} = N + 1$. Let α be a primitive element of $\mathbb{F}_{p^n}$. Then the sequence family is defined as

$$S = \{\mathrm{tr}_1^n(\alpha^{2t+i}) + \mathrm{tr}_1^n(\alpha^{2d(t+k)+j}) | 0 \le i, j \le 1, 0 \le k < N\}.$$

Then the maximum magnitude of the correlation between sequences in S is upper bounded by $\frac{3}{\sqrt{2}}\sqrt{N + \frac{1}{2}} + \frac{1}{2}$. The family size is given as $4N = 2(p^n - 1)$. □

In this chapter, we derive cross-correlation values for $d' = 2d = 4p^{n/2} - 2$, where the original decimation $d = 2p^{n/2} - 1$ was investigated by Helleseth [11]. The original result by Helleseth is given below.

Theorem 4.5 (Helleseth [11])**.** Let p be an odd prime and n be an even integer. Let $p^{n/2} \neq 2 \mod 3$ and $d = 2p^{n/2} - 1$. Then $\gcd(d, p^n - 1) = 1$

and the cross-correlation between $\mathrm{tr}_1^n(\alpha^t)$ and $\mathrm{tr}_1^n(\alpha^{dt})$ takes the following values

(i) $-1-p^{n/2}$ occurs $\frac{1}{3}(p^n-p^{n/2})$ times

(ii) -1 occurs $\frac{1}{2}(p^n-p^{n/2}-2)$ times

(iii) $-1+p^{n/2}$ occurs $p^{n/2}$ times

(iv) $-1+2p^{n/2}$ occurs $\frac{1}{6}(p^n-p^{n/2})$ times. □

The following lemmas are used for derivation of cross-correlation values. These are due to Baumert and McEliece [9] and Helleseth [11].

Lemma 4.6 (Helleseth [11]). Let p be an odd prime and n be an even integer. Then we have

$$\sum_{y\in\mathbb{F}_{p^n}} \omega^{\mathrm{tr}_1^n(ay^{p^{n/2}+1})} = \begin{cases} p^n, & \text{if } a+a^{p^{n/2}}=0 \\ -p^{n/2}, & \text{if } a+a^{p^{n/2}}\neq 0. \end{cases}$$

□

Lemma 4.7 (Helleseth [11]). Let p be an odd prime and n be an integer. Then we have

$$\sum_{y\in\mathbb{F}_{p^n}} \omega^{\mathrm{tr}_1^n(ay^2)}$$
$$= \begin{cases} p^n, & \text{if } a=0 \\ (-1)^{n+1}((-1)^{\frac{p-1}{2}}p)^{n/2}, & \text{if } a \text{ is a square in } \mathbb{F}_{p^n}^* \\ (-1)^n((-1)^{\frac{p-1}{2}}p)^{n/2}, & \text{if } a \text{ is a nonsquare in } \mathbb{F}_{p^n}^*. \end{cases}$$

□

4.3. Correlation Bound

Throughout this section, we use the following notations.

- p is an odd prime.
- $n = 2m$, where m is an integer.
- $d = 2p^{n/2} - 1$ and $d' = 2d = 4p^{n/2} - 2$.
- $N = \frac{p^n-1}{2}$.
- α is a primitive element of $\mathbb{F}_{p^n}$.

Now we determine the correlation values between $m(2t+i)$ and $m(d't+j)$ as in the following theorem.

Theorem 4.8. Let p be an odd prime and $n = 2m$ be an even integer. Let $d' = 2d = 4p^{n/2} - 2$ and $m(t)$ be a p-ary m-sequence of period $p^n - 1$. Then the cross-correlation function between $m(2t + i)$ and $m(d't + j)$, $0 \le i, j \le 1$, takes values in $\left\{ \frac{-1\pm p^{n/2}}{2}, \frac{-1+3p^{n/2}}{2}, \frac{-1+5p^{n/2}}{2} \right\}$.

Proof. The proof can be done using the similar method as in [11] but with some modifications. The correlation function $C_{i,j}(\tau)$ of $m(2t + i)$ and $m(d't + j)$ can be written as

$$C_{i,j}(\tau) = \frac{1}{2} \sum_{x \in \mathbb{F}^*_{p^n}} \omega^{\mathrm{tr}_1^n(ax^2 - bx^{2d})}$$

where $a = \alpha^{2\tau+i}$ and $b = \alpha^j$. Let $x = \alpha^k y^{\frac{p^m+1}{2}}$, $0 \le k < \frac{p^m+1}{2}$, and define the set $C_k = \{z \in \mathbb{F}_{p^n} : z = \alpha^t, t = k \mod \frac{p^m+1}{2}\}$. Then as y runs through all field elements of $\mathbb{F}_{p^n}$, x runs through C_k $\frac{p^m+1}{2}$ times and 0 once. Thus if k takes values from 0 to $\frac{p^m-1}{2}$ and y runs through $\mathbb{F}_{p^n}$, then x runs through $\mathbb{F}_{p^n}$ $\frac{p^m+1}{2}$ times. Since $\frac{p^m+1}{2} d' = p^m + 1 \mod p^n - 1$ and $x = \alpha^k y^{\frac{p^m+1}{2}}$, we have

$$\frac{p^m+1}{2}(C_{i,j}(\tau) + \frac{1}{2}) = \frac{p^m+1}{2}\frac{1}{2} \sum_{x \in \mathbb{F}_{p^n}} \omega^{\mathrm{tr}_1^n(ax^2 - bx^{2d})}$$

$$= \frac{1}{2} \sum_{k=0}^{\frac{p^m-1}{2}} \sum_{y \in \mathbb{F}_{p^n}} \omega^{\mathrm{tr}_1^n(a\alpha^{2k}y^{p^m+1} - b\alpha^{2dk}y^{p^m+1})}$$
$$= \frac{1}{2} \sum_{k=0}^{\frac{p^m-1}{2}} \sum_{y \in \mathbb{F}_{p^n}} \omega^{\mathrm{tr}_1^n(y^{p^m+1}(a\alpha^{2k} - b\alpha^{2dk}))}.$$

Now suppose that $K(a, b)$ is the number of solutions k of

$$(a\alpha^{2k} - b\alpha^{2dk})^{p^m} + a\alpha^{2k} - b\alpha^{2dk} = 0. \tag{4.2}$$

Then by Lemma 4.6, we obtain

$$C_{i,j}(\tau) + \frac{1}{2} = p^m(K(a, b) - \frac{1}{2})$$

and thus

$$C_{i,j}(\tau) = \frac{1}{2}((2K(a, b) - 1)p^m - 1).$$

Therefore it suffices to show that $K(a, b)$ can take only 0, 1, 2, and 3. We consider the following two cases.

1) $p^m = 3 \mod 4$

In this case, we use the following notations:

- $\beta = \alpha^{2(p^m+1)}$ and thus $\beta^{\frac{p^m-1}{2}} = 1$.
- $\gamma = \alpha^{\frac{p^m-1}{2}}$ and thus $\gamma^{2(p^m+1)} = 1$.

Then the followings hold as

- $\gcd(\frac{1}{2}(p^m - 1), 2(p^m + 1)) = 1$
- $\alpha = \beta\gamma$
- $\beta^{p^m} = \beta$
- $\gamma^{p^m} = -\gamma^{-1}$.

By substituting $2k$ by l, we have $2dk = dl$. Then (4.2) can be expressed as

$$\begin{aligned}
&(a\alpha^l - b\alpha^{dl})^{p^m} + a\alpha^l - b\alpha^{dl} \\
&= (a(\beta\gamma)^l - b(\beta\gamma)^{dl})^{p^m} + a(\beta\gamma)^l - b(\beta\gamma)^{dl} \\
&= a^{p^m}\beta^l(-\gamma^{-1})^l - b^{p^m}\beta^{dl}(-\gamma^{-1})^{dl} + a\beta^l\gamma^l - b\beta^{dl}\gamma^{dl}. \qquad (4.3)
\end{aligned}$$

Note that

$$d = 2p^m - 1 = \begin{cases} 1, & \mod \frac{1}{2}(p^m - 1) \\ -3, & \mod 2(p^m + 1). \end{cases}$$

Thus, (4.3) can be rewritten as

$$\begin{aligned}
& a^{p^m}\beta^l\gamma^{-l} - b^{p^m}\beta^l\gamma^{3l} + a\beta^l\gamma^l - b\beta^l\gamma^{-3l} = 0 \\
\Longleftrightarrow\ & a^{p^m}\gamma^{-l} - b^{p^m}\gamma^{3l} + a\gamma^l - b\gamma^{-3l} = 0 \\
\Longleftrightarrow\ & a^{p^m}\gamma^{2l} - b^{p^m}\gamma^{6l} + a\gamma^{4l} - b = 0 \\
\Longleftrightarrow\ & a^{p^m}\gamma^{2l} - b^{p^m}(\gamma^{2l})^3 + a(\gamma^{2l})^2 - b = 0. \qquad (4.4)
\end{aligned}$$

This is the cubic equation of γ^{2l}. Since $l = 2k$, we have $0 \leq l < p^m$. But we have

$$\begin{aligned}
& \gamma^{2l_1} = \gamma^{2l_2} \\
\Longleftrightarrow\ & 2l_1 = 2l_2 \mod 2(p^m + 1) \\
\Longleftrightarrow\ & l_1 = l_2 \mod p^m + 1.
\end{aligned}$$

Therefore, the number of solutions is less than or equal to three. Thus the proof for the case $p^m = 3 \mod 4$ is done.

2) $p^m = 1 \mod 4$:

In this case, the definition for β and γ is modified as follows:

- $\beta = \alpha^{\frac{p^m+1}{2}}$ and thus $\beta^{2(p^m-1)} = 1$.
- $\gamma = \alpha^{2(p^m-1)}$ and thus $\gamma^{\frac{p^m+1}{2}} = 1$.

Then the following properties hold in this case as

- $\gcd(2(p^m-1),\ \frac{1}{2}(p^m+1)) = 1$
- $\alpha = \beta\gamma$
- $\beta^{p^m} = -\beta$
- $\gamma^{p^m} = \gamma^{-1}$.

Using

$$d = 2p^m - 1 = \begin{cases} 1, & \mod 2(p^m-1) \\ -3, & \mod \frac{1}{2}(p^m+1), \end{cases}$$

we have

$$\begin{aligned}
&(a\alpha^l - b\alpha^{dl})^{p^m} + a\alpha^l - b\alpha^{dl} = 0 \\
&\Leftrightarrow a^{p^m}(-\beta)^l\gamma^{-l} - b^{p^m}(-\beta)^l\gamma^{3l} + a\beta^l\gamma^l - b\beta^l\gamma^{-3l} = 0 \\
&\Leftrightarrow a^{p^m}\beta^l\gamma^{-l} - b^{p^m}\beta^l\gamma^{3l} + a\beta^l\gamma^l - b\beta^l\gamma^{-3l} = 0 \\
&\Leftrightarrow a^{p^m}\gamma^{-l} - b^{p^m}\gamma^{3l} + a\gamma^l - b\gamma^{-3l} = 0 \\
&\Leftrightarrow a^{p^m}\gamma^{2l} - b^{p^m}\gamma^{6l} + a\gamma^4 l - b = 0 \\
&\Leftrightarrow a^{p^m}\gamma^{2l} - b^{p^m}(\gamma^{2l})^3 + a(\gamma^{2l})^2 - b = 0. \qquad (4.5)
\end{aligned}$$

This is the cubic equation as in the case of $p^m = 3 \mod 4$. Furthermore, we have

$$\begin{aligned}
&\gamma^{2l_1} = \gamma^{2l_2} \\
\Longleftrightarrow\ & 2l_1 = 2l_2 \mod \frac{1}{2}(p^m+1) \\
\Longleftrightarrow\ & l_1 = l_2 \mod \frac{1}{2}(p^m+1)
\end{aligned}$$

since $\frac{1}{2}(p^m+1)$ is odd. Therefore, the number of solutions is less than or equal to three. Thus the proof is done. □

Remark 4.9. In [11], Helleseth used Theorem 3.8 [11] to derive the equation similar to (4.2). Since we deal with the cross-correlation of two half-period sequences, we cannot directly apply Theorem 3.8 [11] to this case.

Instead, we follow steps similar to the proof of Theorem 3.8 [11] with some modification to accomodate decimations. This technique was also employed in [37] [64]. The idea of considering the cases of $p^m = 3 \mod 4$ and $p^m = 1 \mod 4$ separately is due to Helleseth [11].

Remark 4.10. In [11], the correlation is exactly 4-valued and the value distribution of the cross-correlation is derived. But in this case, the number of the correlation values can be three or four, as proved in Corollary 4.11. Also the technique in [11] cannot be applied to derive the distribution since the correlation considered in this chapter is that of half-period sequences.

In addition, we can obtain the following result for the cross-correlation.

Corollary 4.11. The cross-correlation function between $m(2t+i)$ and $m(d't+j)$, $0 \leq i, j \leq 1$, in Theorem 4.8 takes values in $\left\{\frac{-1 \pm p^{n/2}}{2}, \frac{-1+3p^{n/2}}{2}\right\}$ if

1) $p^m = 3 \mod 4$ and $j = 1$, or

2) $p^m = 1 \mod 4$ and $j = 0$.

Proof. 1) $p^m = 3 \mod 4$ and $j = 1$:

In this case, $b = \alpha^j = \alpha$. Thus (4.4) can be expressed as

$$\begin{aligned} a^{p^m}\gamma^{2l} - b^{p^m}(\gamma^{2l})^3 + a(\gamma^{2l})^2 - b = 0 \\ \Leftrightarrow b^{p^m}(\gamma^{2l})^3 - a(\gamma^{2l})^2 - a^{p^m}\gamma^{2l} + b = 0. \end{aligned}$$

Suppose that three distinct solutions γ^{2l_1}, γ^{2l_2}, and γ^{2l_3} exist. Then we have

$$\gamma^{2l_1}\gamma^{2l_2}\gamma^{2l_3} = \gamma^{2(l_1+l_2+l_3)} = -b^{1-p^m} = \alpha^{\frac{p^n-1}{2}-(p^m-1)}.$$

Therefore

$$\begin{aligned} 2\frac{p^m-1}{2}(l_1+l_2+l_3) = \frac{p^n-1}{2} - (p^m-1) \mod p^n - 1 \\ \Leftrightarrow (l_1+l_2+l_3) = \frac{p^m-1}{2} \mod p^m + 1. \end{aligned}$$

But the left-hand side is even and the right-hand side is odd. Thus the number of solutions of (4.4) is at most 2.

2) $p^m = 1 \mod 4$ and $j = 0$:

Since $p^m = 1 \mod 4$ and $j = 0$, we have $b = 1$. Then (4.5) can be written as

$$\begin{aligned} a^{p^m}\gamma^{2l} - (\gamma^{2l})^3 + a(\gamma^{2l})^2 - 1 = 0 \\ \Leftrightarrow (\gamma^{2l})^3 - a(\gamma^{2l})^2 - a^{p^m}\gamma^{2l} + 1 = 0. \end{aligned}$$

Now suppose that three distinct solutions γ^{2l_1}, γ^{2l_2}, and γ^{2l_3} exist. Then we have

$$\gamma^{2l_1}\gamma^{2l_2}\gamma^{2l_3} = \gamma^{2(l_1+l_2+l_3)} = -1 = \alpha^{\frac{p^n-1}{2}}.$$

Therefore

$$\begin{aligned} 4(p^m-1)(l_1+l_2+l_3) &= \frac{(p^m-1)(p^m+1)}{2} \mod p^n - 1 \\ \Leftrightarrow 4(l_1+l_2+l_3) &= \frac{p^m+1}{2} \mod p^m + 1. \end{aligned}$$

As in the case of 1), the left-hand side is even and the right-hand side is odd. Thus the number of solutions of (4.5) is at most 2. Therefore the proof is complete. □

4.4. Examples

Here are two examples of the theorem and corollary in the previous section.

Example 4.12. First, consider the case $p = 3$, $n = 8$, $i = 1$, $j = 0$, $2d = 322$, that is, $p^m = 1 \mod 4$. Then by numerical computations, the cross-correlation function between $m(2t+1)$ and $m(2dt)$ can be given as

$$C_{1,0}(\tau) = \begin{cases} -41, & 2040 \text{ times} \\ 40, & 840 \text{ times} \\ 121, & 400 \text{ times.} \end{cases}$$

Example 4.13. Now let $p = 7$, $n = 6$, $i = 0$, $j = 0$, $2d = 1370$, that is, $p^m = 3 \mod 4$. By computer experiment, the cross-correlation is given as

$$C_{0,1}(\tau) = \begin{cases} -172, & 34188 \text{ times} \\ 171, & 22120 \text{ times} \\ 514, & 85 \text{ times} \\ 857, & 2431 \text{ times.} \end{cases}$$

One can easily verify that the above examples coincide with the results of Theorem 4.8 and Corollary 4.11.

4.5. A New Sequence Family of Period $\frac{p^n-1}{2}$

Based on Theorem 4.8, a new sequence family of period $\frac{p^n-1}{2}$ can be constructed using shift-and-add method.

Theorem 4.14. Let p be an odd prime and $n = 2m$ be an even integer with $p^m \neq 2 \mod 3$. Suppose $d' = 2d = 4p^{n/2} - 2$ and $m(t)$ is a p-ary m-sequence of period $p^n - 1$. Define the sequence family

$$S = \{s_{i,j,k}(t) = m(2t+i) + m(d'(t+k)+j)\}$$

where $0 \leq i, j \leq 1, 0 \leq k < N = \frac{p^n-1}{2}$. The correlation function of the sequences in S is at most five-valued in $\left\{\frac{p^n-1}{2}, \frac{-1\pm p^{n/2}}{2}, \frac{-1+3p^{n/2}}{2}, \frac{-1+5p^{n/2}}{2}\right\}$, that is, the maximum magnitude of the correlation is upper bounded by $\frac{-1+5p^{n/2}}{2}$ and the family size is $4N = 2(p^n - 1)$.

Proof. Suppose $s_{i_1,j_1,k_1}(t), s_{i_2,j_2,k_2}(t) \in S$. Then the cross-correlation $C(\tau)$ between these two sequences is given as

$$\begin{aligned}
C(\tau) &= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i_1})-\mathrm{tr}_1^n(\alpha^{2t+i_2})+\mathrm{tr}_1^n(\alpha^{d'(t+\tau+k_1)+j_1})-\mathrm{tr}_1^n(\alpha^{d'(t+k_2)+j_2})} \\
&= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i_1}-\alpha^{2t+i_2})+\mathrm{tr}_1^n(\alpha^{d'(t+\tau+k_1)+j_1}-\alpha^{d'(t+k_2)+j_2})} \\
&= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n((\alpha^{2\tau+i_1}-\alpha^{i_2})\alpha^{2t})+\mathrm{tr}_1^n((\alpha^{(d'(\tau+k_1)+j_1}-\alpha^{d'k_2+j_2})\alpha^{d't})} \\
&= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(a\alpha^{2t}-b\alpha^{d't})}
\end{aligned}$$

where $a = \alpha^{2\tau+i_1} - \alpha^{i_2}$ and $b = \alpha^{d'(\tau+k_1)+j_1} - \alpha^{d'k_2+j_2}$. But this is the same form as the cross-correlation between $m(2t+i)$ and $m(d't+j)$ in Theorem 3 if $a \neq 0$ and $b \neq 0$. If $a = b = 0$, then $\tau = 0, i_1 = i_2, j_1 = j_2$, and $k_1 = k_2$, which implies the in-phase autocorrelation. If $a = 0, b \neq 0$ or $a \neq 0, b = 0$, then by Lemma 4.7, the correlation value is $\frac{-1\pm p^m}{2}$. Therefore, the maximum magnitude of the correlation is upper bounded by $\frac{-1+5p^{n/2}}{2}$. Also it is easily checked that the family size of S is $4N$ since $p^m \neq 2 \mod 3$ implies $\gcd(p^n-1,\, d) = 1$. Therefore the proof is complete. □

Note that the condition $p^m \neq 2 \mod 3$ is not too restrictive because $p^m = 2 \mod 3$ is equivalent to $p = 2 \mod 3$ and m is odd. Thus we can construct the proposed family if $p = 1 \mod 3$ or m is even. For comparison, some known half-period sequence families are listed in Table 4.2.

4.6. Discussions

To derive the distribution of the cross-correlation, generally we need to compute $\sum_{\tau=0}^{N-1} C_{i,j}(\tau)$, $\sum_{\tau=0}^{N-1} C_{i,j}(\tau)^2$, $\sum_{\tau=0}^{N-1} C_{i,j}(\tau)^3$ because the correlation is at most 4-valued. In the case of Corollary 4.11 where the number of the correlation values is three, only $\sum_{\tau=0}^{N-1} C_{i,j}(\tau) and \sum_{\tau=0}^{N-1} C_{i,j}(\tau)^2$ are needed. The summation $\sum_{\tau=0}^{N-1} C_{i,j}(\tau)$ is easily obtained, but $\sum_{\tau=0}^{N-1} C_{i,j}(\tau)^2$ is not. This problem will be discussed below.

Lemma 4.15. For $p^m = 1 \mod 4$ and $p^m \neq 2 \mod 3$, the cross-correlation function $C_{i,0}(\tau)$ between $m(2t+i)$ and $m(d't+j)$, $0 \leq i \leq 1, j = 0$, in Theorem 4.8 satisfies

$$\sum_{\tau=0}^{N-1} C_i(\tau) = \begin{cases} \frac{1}{2}(-p^m-1)^2, & i=0 \\ \frac{1}{2}(p^m-1)(p^m+1), & i=1. \end{cases}$$

Proof. We have

$$\sum_{\tau=0}^{N-1} C_i(\tau) = \frac{1}{2}\sum_{\tau=0}^{N-1}\sum_{x\in\mathbb{F}_{p^n}^*} \omega^{\mathrm{tr}_1^n(ax^2-bx^{2d})} = \frac{1}{2}\sum_{x\in\mathbb{F}_{p^n}^*} \omega^{-\mathrm{tr}_1^n(bx^{2d})} \sum_{\tau=0}^{N-1} \omega^{\mathrm{tr}_1^n(ax^2)}.$$

Letting $y = \alpha^\tau$ and $a = y^2\alpha^i$, it follows that

$$\sum_{\tau=0}^{N-1} \omega^{\mathrm{tr}_1^n(ax^2)} = \frac{1}{2}\sum_{y\in\mathbb{F}_{p^n}^*} \omega^{\mathrm{tr}_1^n(y^2\alpha^i x^2)} \begin{cases} \frac{1}{2}(-p^m-1), & i=0 \\ \frac{1}{2}(p^m-1), & i=1 \end{cases}$$

by Lemma 4.7. Also, note that

$$\sum_{x\in\mathbb{F}_{p^n}^*} \omega^{-\mathrm{tr}_1^n(bx^{2d})} = \sum_{x\in\mathbb{F}_{p^n}^*} \omega^{\mathrm{tr}_1^n(-bx^2)} = \sum_{x\in\mathbb{F}_{p^n}^*} \omega^{\mathrm{tr}_1^n(-x^2)} = -p^m-1$$

since $\gcd(2d, p^n-1) = 2$ and -1 is a square. Thus,

$$\sum_{\tau=0}^{N-1} C_i(\tau) = \begin{cases} \frac{1}{2}(-p^m-1)^2, & i=0 \\ \frac{1}{2}(p^m-1)(p^m+1), & i=1. \end{cases}$$

□

Now we deal with the second moment of the correlation, $\sum_{\tau=0}^{N-1} C_{i,j}(\tau)^2$.

For this, we need the following result [66] [64]. Here QR and QNR are sets of squares and nonsquares of $\mathbb{F}_{p^n}$, respectively.

Lemma 4.16 (Dickson [66])**.** Let $z \in \mathbb{F}_{p^n}^*$. Then if -1 is a square, we have

$$1 + z^2 \in \begin{cases} \{0\}, & 2 \text{ times} \\ QR, & \frac{p^n-5}{2} \text{ times} \\ QNR, & \frac{p^n-1}{2} \text{ times.} \end{cases}$$

When -1 is a nonsquare, we have

$$1 + z^2 \in \begin{cases} \{0\}, & 0 \text{ times} \\ QR, & \frac{p^n-3}{2} \text{ times} \\ QNR, & \frac{p^n+1}{2} \text{ times.} \end{cases}$$

□

Now we define N_1, N_2, N_3, N_4 as

$$N_1 = |\{z \in \mathbb{F}_{p^n}^* : 1 + z^2 \in QR, 1 + z^{2d} \in QR\}|$$

$$N_2 = |\{z \in \mathbb{F}_{p^n}^* : 1 + z^2 \in QR, 1 + z^{2d} \in QNR\}|$$

$$N_3 = |\{z \in \mathbb{F}_{p^n}^* : 1 + z^2 \in QNR, 1 + z^{2d} \in QR\}|$$

$$N_4 = |\{z \in \mathbb{F}_{p^n}^* : 1 + z^2 \in QNR, 1 + z^{2d} \in QNR\}|.$$

Then we have the following result.

Lemma 4.17. For $p^m = 1 \mod 4$ and $p^m \neq 2 \mod 3$, the cross-correlation function $C_{0,0}(\tau)$ between $m(2t+i)$ and $m(d't+j)$ for $i = 0, j = 0$ in Theorem 4.8 satisfies

$$\sum_{\tau=0}^{N-1} C_{0,0}(\tau)^2$$

$$= \frac{1}{8}[2(p^n-1)^2 - 4p^m + p^n - 3 + p^n(N_1 + N_4 - N_2 - N_3)].$$

Proof. We have

$$\sum_{\tau=0}^{N-1} C_{0,0}(\tau)^2 = \frac{1}{4}\sum_{\tau=0}^{N-1}\sum_{x_1\in\mathbb{F}_{p^n}^*}\omega^{\mathrm{tr}_1^n(ax_1^2-x_1^{2d})}\sum_{x_2\in\mathbb{F}_{p^n}^*}\omega^{\mathrm{tr}_1^n(ax_2^2-x_2^{2d})}.$$

Let $a=\alpha^{2\tau}$ and $y=\alpha^\tau$. Thus $\alpha^{2\tau}=y^2=a$. Then,

$$\begin{aligned}\sum_{\tau=0}^{N-1} C_{0,0}(\tau)^2 &= \frac{1}{4}\sum_{x_1\in\mathbb{F}_{p^n}^*}\sum_{x_2\in\mathbb{F}_{p^n}^*}\omega^{-\mathrm{tr}_1^n(x_1^{2d}+x_2^{2d})}\frac{1}{2}\sum_{y\in\mathbb{F}_{p^n}^*}\omega^{\mathrm{tr}_1^n(y^2(x_1^2+x_2^2))}\\ &= \frac{1}{8}\sum_{x_1\in\mathbb{F}_{p^n}^*}\sum_{x_2\in\mathbb{F}_{p^n}^*}\omega^{-\mathrm{tr}_1^n(x_1^{2d}+x_2^{2d})}\sum_{y\in\mathbb{F}_{p^n}^*}\omega^{\mathrm{tr}_1^n(y^2(x_1^2+x_2^2))}\\ &= \frac{1}{8}\sum_{x_1\in\mathbb{F}_{p^n}^*}\sum_{z\in\mathbb{F}_{p^n}^*}\omega^{-\mathrm{tr}_1^n(x_1^{2d}(1+z^{2d}))}\sum_{y\in\mathbb{F}_{p^n}^*}\omega^{\mathrm{tr}_1^n(y^2x_1^2(1+z^2))}\end{aligned}$$

where we take $z=x_2/x_1$. Define

$$X(x_1,z)=\omega^{-\mathrm{tr}_1^n(x^2d_1(1+z^{2d}))}\sum_{y\in\mathbb{F}_{p^n}^*}\omega^{\mathrm{tr}_1^n(y^2x_1^2(1+z^2))}.$$

Then we have

$$\begin{aligned}\sum_{\tau=0}^{N-1} C_{0,0}(\tau)^2 = \frac{1}{8}\sum_{x_1\in\mathbb{F}_{p^n}^*}\Bigg[&\sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2=0}} X(x_1,z) + \sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2\,\in\, QR}} X(x_1,z)\\ &+ \sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2\,\in\, QNR}} X(x_1,z)\Bigg].\end{aligned}$$

Since $(d,p^n-1)=1$, we have $1+z^2=0 \Leftrightarrow 1+z^{2d}=0$. Therefore,

$$\sum_{x_1\in\mathbb{F}_{p^n}^*}\sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2=0}} X(x_1,z)$$

$$
\begin{aligned}
&= \sum_{x_1 \in \mathbb{F}_{p^n}^*} \sum_{\substack{z \in \mathbb{F}_{p^n}^* \\ 1+z^2=0}} \omega^{-\mathrm{tr}_1^n(x_1^{2d}(1+z^{2d}))} \sum_{y \in \mathbb{F}_{p^n}^*} \omega^{\mathrm{tr}_1^n(y^2 x_1^2(1+z^2))} \\
&= \sum_{x_1 \in \mathbb{F}_{p^n}^*} \sum_{\substack{z \in \mathbb{F}_{p^n}^* \\ 1+z^2=0}} \omega^{-\mathrm{tr}_1^n(x_1^{2d}(1+z^{2d}))} (p^n-1) = 2(p^n-1)^2.
\end{aligned}
$$

Thus, we have

$$
\begin{aligned}
&\sum_{x_1 \in \mathbb{F}_{p^n}^*} \sum_{\substack{z \in \mathbb{F}_{p^n}^* \\ 1+z^2 \in QR}} X(x_1, z) \\
&\qquad = \sum_{x_1 \in \mathbb{F}_{p^n}^*} \sum_{\substack{z \in \mathbb{F}_{p^n}^* \\ 1+z^2 \in QR}} \omega^{-\mathrm{tr}_1^n(x_1^{2d}(1+z^{2d}))} \sum_{y \in \mathbb{F}_{p^n}^*} \omega^{\mathrm{tr}_1^n(y^2 x_1^2(1+z^2))} \\
&\qquad = \sum_{x_1 \in \mathbb{F}_{p^n}^*} \sum_{\substack{z \in \mathbb{F}_{p^n}^* \\ 1+z^2 \in QR}} \omega^{-\mathrm{tr}_1^n(x_1^{2d}(1+z^{2d}))} (-p^m-1) \\
&\qquad =(-p^m-1) \sum_{x_1 \in \mathbb{F}_{p^n}^*} \sum_{\substack{z \in \mathbb{F}_{p^n}^* \\ 1+z^2 \in QR}} \omega^{-\mathrm{tr}_1^n(x_1^{2d}(1+z^{2d}))} \\
&\qquad =(-p^m-1) \sum_{x_1 \in \mathbb{F}_{p^n}^*} \sum_{\substack{z \in \mathbb{F}_{p^n}^* \\ 1+z^2 \in QR \\ 1+z^{2d} \in QR}} \omega^{-\mathrm{tr}_1^n(x_1^{2d}(1+z^{2d}))} \\
&\qquad\quad + (-p^m-1) \sum_{x_1 \in \mathbb{F}_{p^n}^*} \sum_{\substack{z \in \mathbb{F}_{p^n}^* \\ 1+z^2 \in QR \\ 1+z^{2d} \in QNR}} \omega^{-\mathrm{tr}_1^n(x_1^{2d}(1+z^{2d}))} \\
&\qquad =(-p^m-1) \sum_{x_1 \in \mathbb{F}_{p^n}^*} \sum_{\substack{z \in \mathbb{F}_{p^n}^* \\ 1+z^2 \in QR \\ 1+z^{2d} \in QR}} (-p^m-1) \\
&\qquad\quad + (-p^m-1) \sum_{x_1 \in \mathbb{F}_{p^n}^*} \sum_{\substack{z \in \mathbb{F}_{p^n}^* \\ 1+z^2 \in QR \\ 1+z^{2d} \in QNR}} (p^m-1) \\
&\qquad =(-p^m-1)^2 N_1 + (-p^m-1)(p^m-1) N_2.
\end{aligned}
$$

Likewise,

$$\sum_{x_1\in\mathbb{F}_{p^n}^*}\sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2\,\in\,QNR}} X(x_1,z)$$

$$\begin{aligned}
&=\sum_{x_1\in\mathbb{F}_{p^n}^*}\sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2\,\in\,QNR}} \omega^{-\mathrm{tr}_1^n(x_1^{2d}(1+z^{2d}))}\sum_{y\in\mathbb{F}_{p^n}^*}\omega^{\mathrm{tr}_1^n(y^2x_1^2(1+z^2))}\\
&=\sum_{x_1\in\mathbb{F}_{p^n}^*}\sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2\,\in\,QNR}} \omega^{-\mathrm{tr}_1^n(x_1^{2d}(1+z^{2d}))}(p^m-1)\\
&=(p^m-1)\sum_{x_1\in\mathbb{F}_{p^n}^*}\sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2\,\in\,QNR}} \omega^{-\mathrm{tr}_1^n(x_1^{2d}(1+z^{2d}))}\\
&=(p^m-1)\sum_{x_1\in\mathbb{F}_{p^n}^*}\sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2\,\in\,QNR\\ 1+z^{2d}\,\in\,QR}} \omega^{-\mathrm{tr}_1^n(x_1^{2d}(1+z^{2d}))}\\
&\quad+(p^m-1)\sum_{x_1\in\mathbb{F}_{p^n}^*}\sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2\,\in\,QNR\\ 1+z^{2d}\,\in\,QNR}} \omega^{-\mathrm{tr}_1^n(x_1^{2d}(1+z^{2d}))}\\
&=(p^m-1)\sum_{x_1\in\mathbb{F}_{p^n}^*}\sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2\,\in\,QNR\\ 1+z^{2d}\,\in\,QR}} (-p^m-1)\\
&\quad+(p^m-1)\sum_{x_1\in\mathbb{F}_{p^n}^*}\sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2\,\in\,QNR\\ 1+z^{2d}\,\in\,QNR}} (p^m-1)\\
&=(p^m-1)(-p^m-1)N_3+(p^m-1)^2N_4.
\end{aligned}$$

Therefore, combining these results, we have

$$\sum_{\tau=0}^{N-1}C_{0,0}(\tau)^2=\frac{1}{8}\sum_{x_1\in\mathbb{F}_{p^n}^*}\Bigg[\sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2\,=\,0}} X(x_1,z)+\sum_{\substack{z\,\in\,\mathbb{F}_{p^n}^*\\ 1+z^2\,\in\,QR}} X(x_1,z)$$

$$+ \sum_{\substack{z \in \mathbb{F}_{p^n}^* \\ 1+z^2 \in QNR}} X(x_1, z)\Bigg]$$

$$= \frac{1}{8}[2(p^n-1)^2 - 4p^m + p^n - 3 + p^n(N_1 + N_4 - N_2 - N_3)].$$

□

Therefore, we compute N_1, N_2, N_3, N_4 and then $\sum_{\tau=0}^{N-1} C_{0,0}(\tau)^2$ is obtained, and thus we can derive the distribution for the case $p^m = 1 \mod 4, i = 0, j = 0$. From Lemma 4.16, we can show that $N_2 = N_3$ and $N_1 + 2 = N_4$. Thus, we need one more equation over N_1, N_2, N_3, N_4 to do this. But evaluation of these numbers does not seem to be easy. Thus we remain it as a further work.

In Table 4.3, values of N_1, N_2, N_3, N_4 are tabulated for some parameters p, n, and m. Note that relations $N_2 = N_3$ and $N_1 + 2 = N_4$ are valid for $p^m \neq 2 \mod 3$ cases. But for $p = 5$ and $n = 6$, we have $p^m = 125 = 2 \mod 3$. One can check that $N_2 \neq N_3$ and $N_1 + 2 \neq N_4$ in this case.

4.7. Conclusion

In this chapter, for any odd prime p and an even integer $n = 2m$, the cross-correlation values between two decimated m-sequences by 2 and $d' = 4p^{n/2} - 2$ are determined. The cross-correlation is at most 4-valued and takes values in $\left\{\frac{-1\pm p^{n/2}}{2}, \frac{-1+3p^{n/2}}{2}, \frac{-1+5p^{n/2}}{2}\right\}$. Based on this, for $p^m \neq 2 \mod 3$, a new half-period sequence family is constructed by the shift-and-add method. The maximum magnitude of the correlation values of the sequences in the family is upper bounded by $\frac{-1+5p^{n/2}}{2}$ and the family size

Table 4.3: Values of N_1, N_2, N_3, N_4.

p	n	m	p^m	N_1	N_2	N_3	N_4
3	4	2	$1 \mod 4$	22	16	16	24
	6	3	$3 \mod 4$	194	168	168	196
	8	4	$1 \mod 4$	1678	1600	1600	1680
	10	5	$3 \mod 4$	14882	14640	14640	14884
5	4	2	$1 \mod 4$	182	128	128	184
	6	3	$1 \mod 4$	4018	3792	4040	3768
	8	4	$1 \mod 4$	98286	97024	97024	98288
7	4	2	$1 \mod 4$	606	592	592	608
	6	3	$3 \mod 4$	29510	29312	29312	29512
11	4	2	$1 \mod 4$	3782	3536	3536	3784
13	4	2	$1 \mod 4$	7270	7008	7008	7272

is 4 times of the period of sequences, $4N$.

Chapter 5. On the Cross-Correlation of Ternary m-Sequences of Period $3^{4k+2}-1$ with Decimation $\frac{3^{4k+2}-3^{2k+1}+2}{4}+3^{2k+1}$

In this chapter, for an integer k, we evaluate an upper bound on the cross-correlation of a ternary m-sequence of period $N = 3^{4k+2}-1$ and its decimated sequence with decimation $d = \frac{3^{4k+2}-3^{2k+1}+2}{4}+3^{2k+1}$. It is found that the cross-correlation is upper bounded by $4.5 \cdot 3^{2k+1}+1$. To prove this, we use the quadratic form theory. Unlike the previous works, we have four quadratic forms involved, and using Bluher's result [33], we restrict the number of zeros of linearized polynomials by 1, 9, and 81. Also we prove that among four linearized polynomials, at most one polynomial can have 81 zeros. [1]

5.1. Introduction

The cross-correlation between p-ary m-sequences and their decimated sequences by d has been extensively studied by many researchers. Trachtenberg [7] investigated the cross-correlation for the decimation $d = \frac{p^k+2}{2}$

[1] The material of this chapter is primarily based on the following proceeding: ©2012 IEEE. Reprinted, with permission, from Ji-Youp Kim, Sung-Tai Choi, Taehyung Lim, Jong-Seon No, and Habong Chung, "On the cross-correlation of ternary m-sequences of period $3^{4k+2}-1$ with decimation $(3^{4k+2}-3^{2k+1}+2)/4+3^{2k+1}$," *IEEE International Symposium on Information Theory*, Cambridge, MA, Jul. 2012

and $d = p^{2k} - p^k + 1$ when p is an odd prime. Helleseth [11] summarized many known results and evaluated cross-correlation distributions for various values of decimations. Muller [27] proved that for odd n, the cross-correlation between a ternary m-sequence and its decimation by $d = \frac{3^n+1}{3+1} + \frac{3^n-1}{2}$ is upper bounded by $2\sqrt{p^n}$. Hu, Li, Mills, Muller, Sun, Willems, Yang, and Zhang [28] generalized Muller's result to $p = 3 \bmod 4$, and Xia, Zeng, and Hu [46] have evaluated the correlation distribution. More recently, Ness, Helleseth, and Kholosha [34] derived the distribution of the cross-correlation values for $p = 3$, $d = \frac{3^k+1}{2}$, where k is an odd integer with $\gcd(k, n) = 1$. For an odd prime p, even n, and $d = p^k + 1$ with $\gcd(n, k) = 1$, Seo, Kim, No, and Shin [36] estimated the upper bound $1 + p\sqrt{p^n}$. Choi, Lim, No, and Chung [52] investigated cross-correlation values for an odd prime p and decimation $d = \frac{(p^m+1)^2}{2(p+1)}$, where m is odd. For a more detailed overview on this subject, we refer the reader to [54].

In this chapter, for an integer k, we derived an upper bound on the cross-correlation of a ternary m-sequence of period $3^{4k+2} - 1$ and its decimation with $d = \frac{3^{4k+2}-3^{2k+1}+2}{4} + 3^{2k+1}$. It is shown that the upper bound is given as $4.5 \cdot 3^{2k+1} + 1$. For the derivation, we use the quadratic form theory as in [27] [28] [34] [36] [46] [52], but in this case four quadratic forms are involved. To obtain possible rank combinations of quadratic forms, Bluher's result [33] [35] is employed. It is shown that quadratic forms have only even ranks and among four quadratic forms, at most one of them has the lowest rank.

The remainder of this chapter is organized as follows. In Section 5.2, we introduce the basic facts for the quadratic forms and linearized polynomials. In Section 5.3, we present the Bluher's result [33]. In Section 5.4, we collect notations and explain the step of the proof. In Section 5.5, we discuss how to transform the cross-correlation into the quadratic form. Next, we investigate the possible rank combination of quadratic forms in Section 5.6. In Section 5.7, we derive the upper bound on the cross-correlation magnitude. Some examples are given in Section 5.8 and the related result by Xia, Chen, Hellseth, and Li [49] is introduced in Section 5.9. Finally, concluding remarks are given in Section 5.10.

5.2. Quadratic Forms and Linearized Polynomials

In this section, we introduce the *quadratic form*, which is the main tool for analyzing the cross-correlation in this chapter. Also, linearized polynomials, whose zero sets are the kernels of corresponding quadratic forms, are defined. The following discussion can be found in [72] [73].

Let V be an n-dimensional vector space over the field F. We can define a bilinear form B as follows.

Definition 5.1 (Bilinear forms [73])**.** A bilinear form B is a function $B : V \times V \rightarrow F$ such that

(1) $B(ax + by, z) = aB(x, z) + bB(y, z)$ for all $x, y, z \in V$ and $a, b \in F$

(2) $B(x, ay + bz) = aB(x, y) + bB(x, z)$ for all $x, y, z \in V$ and $a, b \in F$. □

That is, the bilinear form is linear for each argument. Let $\mathcal{B} = \{v_1, ..., v_n\}$ be an ordered basis of V. Then we can map the bilinear form B to its associated matrix $[B]_{\mathcal{B}}$ as

$$[B]_{\mathcal{B}} = \big(B(v_i, v_j)\big).$$

Thus each (i, j) component of $[B]_{\mathcal{B}}$ is $B(v_i, v_j)$. Conversely, for each $n \times n$ matrix J over F, we can define the bilinear form $B_E^J : F^n \times F^n \to F$ as

$$B_E^J(x, y) = x^T Jy$$

where $x, y \in F^n$ and E is a standard basis of F. It is immediate that B_E^J is indeed a bilinear form on F^n.

One can show that the set of all bilinear form over V and the set of all $n \times n$ matrices over F are vector spaces over F. Furthermore, it is easily shown that these are isomorphic each other by the mapping

$$B \longmapsto [B]_{\mathcal{B}}.$$

Symmetric bilinear forms are of particular interest to us.

Definition 5.2 (Symmetric bilinear forms [73])**.** A bilinear form B is called symmetric if

$$B(x, y) = B(y, x) \text{ for all } x, y \in V.$$

□

For example, the inner product defined on the Euclidean space $\mathbb{R}^n$ is a special case of symmetric bilinear forms.

Now we define the quadratic form.

Definition 5.3 (Quadratic forms [73])**.** Let V be a finite dimensional vector space over the field F. Then the function $Q : V \to F$ is quadratic form over V if

(1) Let $B_Q : V \times V \to F$ be the function defined by

$$B_Q(v, w) = Q(v + w) - Q(v) - Q(w)$$

where $v, w \in V$. Then B_Q is a bilinear form over V.

(2) For all $v \in V, c \in F$, we have

$$Q(cv) = c^2 Q(v).$$

□

Therefore, if we are given the quadratic form, then we have the associated bilinear form. The converse is also true.

Lemma 5.4 (Exercise 14.2.3 [73])**.** Let B be a symmetric bilinear form over the finite dimensional vector space V over the field F. Let $Q : V \to F$ be the function defined by

$$2Q(v) = B(v, v)$$

where $v \in V$. Then Q is a quadratic form over V. Furthermore, we have $B = B_Q$. □

Thus we can say that quadratic forms and symmetric bilinear forms are equivalent. Furthermore, quadratic forms can be expressed as quadratic equations over F. Suppose Q is a quadratic form over V and let $\mathcal{B} = \{v_1, ..., v_n\}$ be an ordered basis of V. Then we can find the symmetric matrix $J = (a_{ij})$ such that $B_Q = B^J_{\mathcal{B}}$. For each $v = \sum_{i=1}^{n} x_i v_i \in V$, let

$[v]_{\mathcal{B}} = (x_1, ..., x_n)^T$. Then we have

$$2Q(v) = B_Q(v, v) = [v]_{\mathcal{B}}^T J[v]_{\mathcal{B}} = \sum_{i,j} a_{ij}x_ix_j.$$

Therefore, $Q(v)$ is a quadratic equation of $x_1, ..., x_n$. Conversely, consider a quadratic equation

$$2Q(x_1, ..., x_n) = \sum_{i,j} a_{ij}x_ix_j$$

where $a_{ij} = a_{ji}$. Let $v, w \in V$ such that $[v]_{\mathcal{B}} = (x_1, ..., x_n)^T, [w]_{\mathcal{B}} = (y_1, ..., y_n)^T$ and $Q(v) = Q(x_1, ..., x_n)$. Then,

$$\begin{aligned} 2B_Q(v, w) &= 2Q(v + w) - Q(v) - Q(w) \\ &= \sum_{i,j} a_{ij}(x_i + y_i)(x_j + y_j) \\ &- \sum_{i,j} a_{ij}x_ix_j - \sum_{i,j} a_{ij}y_iy_j \\ &= 2\sum_{i,j} a_{ij}x_iy_j. \end{aligned}$$

Therefore, by letting $J = (a_{ij})$, J is symmetric and

$$B_Q(v, w) = \sum_{i,j} x_ia_{ij}y_j = [v]_{\mathcal{B}}^T J[w]_{\mathcal{B}}.$$

Thus B_Q is a bilinear form over V. Therefore, Q is a quadratic form over V. This implies that quadratic forms are equivalent to quadratic equations. In this case, (V, B) or simply V, is called a quadratic space.

In this chapter, we deal with the problem of finding the dimension of kernels of bilinear forms.

Definition 5.5 (Kernels of bilinear forms [72])**.** Let B be a bilinear form of a vector space V. Then the left kernel of B is defined as

$$\{v \in V | B(v, x) = 0 \text{ for all } x \in x\}$$

and the right kernel of B is similarly defined as

$$\{v \in V | B(x, v) = 0 \text{ for all } x \in x\}.$$

□

The computation of dimensions of these kernels is important to calculate the correlation bound. Note that if a bilinear form is symmetric, then its left kernel and right kernel are equal. In this case, the left kernel and the right kernel are simply called the kernel and denoted by $V^{\perp}$. If $V^{\perp}$ is a zero vector space, then we call V a nondegenerate quadratic space and its bilinear form nondegenerate. The rank of a bilinear form is $\dim(V) - \dim(V^{\perp})$. Therefore, the rank of a nondegenerate bilinear form is always the full dimension.

In this chapter, we deal with the quadratic forms defined over the finite field. For a prime p and an integer n, let $\mathbb{F}_{p^n}$ be the finite field of p^n elements. Since $\mathbb{F}_{p^n}$ is a n-dimensional vector space over $\mathbb{F}_p$, we identify $\mathbb{F}_{p^n}$ as $\mathbb{F}_p^n$. Then a quadratic form f over $\mathbb{F}_{p^n}$ is expressed by a homogeneous polynomial of degree 2 in $\mathbb{F}_p[x_1, ..., x_n]$. That is,

$$f(x_1, x_2, ..., x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$$

where $a_{ij} \in \mathbb{F}_p$. The matrix $A = (a_{ij})$ is called a coefficient matrix of f and $\det(f) = \Delta$ is defined to be $\det(A)$. If the rank of A is k for some

$0 \leq k \leq n$, then it follows that the rank of f is also k. If $\text{rank}(f) = n$, then f is nondegenerate [70].

A quadratic character $\eta(x)$ of $\mathbb{F}_{p^n}$ is defined as

$$\eta(x) = \begin{cases} 1, & \text{if } x \text{ is a nonzero square in } \mathbb{F}_{p^n} \\ -1, & \text{if } x \text{ is a nonzero nonsquare in } \mathbb{F}_{p^n} \\ 0, & \text{if } x = 0. \end{cases}$$

For a nondegenerate quadratic form f over $\mathbb{F}_p$, one can calculate the number of solutions of $f(x_1, x_2, ..., x_n) = b$ for $b \in \mathbb{F}_p$ by the following lemma.

Lemma 5.6 (Theorem 6.26, 6.27 [70])**.** Let η be the quadratic character of $\mathbb{F}_p$. The number of solutions $N(b)$ of $f(x_1, x_2, ..., x_n) = b$ in $\mathbb{F}_p^n$, when f is a nondegenerate quadratic form of rank n with determinant Δ and $b \in \mathbb{F}_p$, is given as follows:
Case 1) n even;

$$N(b) = \begin{cases} p^{n-1} - \epsilon p^{\frac{n-2}{2}}, & \text{if } b \neq 0 \\ p^{n-1} - \epsilon(p-1)p^{\frac{n-2}{2}}, & \text{if } b = 0 \end{cases}$$

where $\epsilon = \eta((-1)^{n/2}\Delta)$.
Case 2) n odd;

$$N(b) = \begin{cases} p^{n-1} + \epsilon\eta(b)p^{\frac{n-1}{2}}, & \text{if } b \neq 0 \\ p^{n-1}, & \text{if } b = 0 \end{cases}$$

where $\epsilon = \eta((-1)^{(k-1)/2}\Delta)$. □

From Lemma 5.6, the following lemma is easily derived.

Lemma 5.7 (Ness, Helleseth, and Kholosha [34])**.** Let η be the quadratic character of $\mathbb{F}_3$. Let f be a nondegenerate quadratic form in n variables with determinant Δ and ω be the 3rd root of unity. Then

$$S = \sum_{x \in \mathbb{F}_{3^n}} \omega^{f(x)}$$

is given by

$$S = \begin{cases} \epsilon 3^{n/2}, & \text{if } n \text{ is even} \\ \epsilon \sqrt{-1} 3^{n/2}, & \text{if } n \text{ is odd} \end{cases}$$

where $\epsilon = \eta((-1)^{n/2}\Delta)$ for even n and $\epsilon = \eta((-1)^{(n-1)/2}\Delta)$ for odd n. □

For the case of rank$(f) = k < n$, we can obtain the number of solutions by multiplying the result of Lemma 5.6 or Lemma 5.7 by p^{n-k}. Since the rank of quadratic form can be computed from the dimension of the kernel, we have:

Lemma 5.8 (Muller [27]). Let $f \in \mathbb{F}_p[x_1, x_2, ..., x_n]$ be a quadratic form. Define

$$Z = \{z \in \mathbb{F}_p^n : f(x+z) - f(x) = 0 \text{ for all } x \in \mathbb{F}_p^n\}.$$

Then Z is a subspace of $\mathbb{F}_p^n$ and rank$(f) = n - \dim(Z)$. □

Note that Z is the kernel of f.

Let q be a prime power and m be an integer. A polynomial of the form

$$L(x) = \sum_i a_i x^{q^i}$$

with coefficients in $\mathbb{F}_{q^m}$ is called a linearized polynomial over $\mathbb{F}_{q^m}$. For an extension field F of $\mathbb{F}_{q^m}$, we have

$$L(x+y) = L(x) + L(y), \text{ for all } x, y \in F$$

$$L(cx) = cL(x), \text{ for all } x \in F \text{ and } c \in \mathbb{F}_q.$$

Thus the set of roots of a linearized polynomial is a vector space over $\mathbb{F}_q$ and the number of roots is a power of q.

5.3. Number of Solutions of $x^{p^s+1} - cx + c$

The following lemmas will be used to determine the number of solutions of some linearized polynomials.

Lemma 5.9 (Bluher [33], Zeng, Li, and Hu [35])**.** Let $h_c(x) = x^{p^s+1} - cx + c$, $c \in \mathbb{F}_{p^n}^*$. Then $h_c(x) = 0$ has either 0, 1, 2, or $p^{\gcd(s,n)} + 1$ roots in $\mathbb{F}_{p^n}^*$. □

Lemma 5.10 (Bluher [33])**.** Let F be a finite field of characteristic p and $c \in F^*$. Suppose q is a power of p and $F \cap \mathbb{F}_q = \mathbb{F}_Q$. Define $f(x) = x^{q+1} - cx + c$. Then the following are equivalent:

1) f has at least three roots in F;

2) f has exactly $Q + 1$ roots in F;

3) f has at least two roots in F and $N_{F/\mathbb{F}_Q}(r - 1) = 1$ for all root r in F.

□

By setting $F = \mathbb{F}_{p^{4k+2}}$ and $q = p^{2k}$ in Lemma 5.10, we have the following result.

Corollary 5.11. Let k be an integer, $n = 4k+2$, and p be an odd prime. Then $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^{2k}} = \mathbb{F}_{p^2}$. Let $f(x) = x^{p^{2k}+1} - cx + c$, $c \in \mathbb{F}_{p^n}^*$. Then the following are equivalent.

1) f has exactly $p^2 + 1$ roots in $\mathbb{F}_{p^n}$;

2) f has at least two roots in $\mathbb{F}_{p^n}$ and

$$(r-1)^{\frac{p^n-1}{p^2-1}} = 1$$

for all root r in $\mathbb{F}_{p^n}$. □

5.4. Notations

First we collect notations here.

- k is an integer;
- $n = 2m = 2 + 4k$;
- $d = \frac{3^n - 3^m + 2}{4} + 3^m$;
- $\mathbb{F}_{3^n}$ is the finite field with 3^n elements;
- α is a primitive element of $\mathbb{F}_{3^n}$;
- $N = 3^n - 1$;
- $\gcd(N, d) = \frac{3^m+1}{4}$;
- $0 \leq l < \gcd(N, d)$.

In continuing sections, we derive the cross-correlation function $C(\tau)$ between $\mathrm{tr}_1^n(\alpha^t)$ and $\mathrm{tr}_1^n(\alpha^{dt+l})$ with time shift τ. To do this, we follow steps introduced below [54]:

(1) Transform the correlation function into the exponential sums of quadratic form exponents.

(2) Obtain the possible ranks and rank combinations of quadratic forms.

(3) Using Lemma 5.6, calculate the upper bound on the correlation.

First, we attempt to transform the cross-correlation into the quadratic form.

5.5. Quadratic Form Expression of the Cross-Correlation Function

In this section, we transform the cross-correlation function $C(\tau)$ between $\mathrm{tr}_1^n(\alpha^t)$ and $\mathrm{tr}_1^n(\alpha^{dt+l})$ with time shift τ into the exponential sum with a quadratic form exponent.

$C(\tau)$ is given as

$$\begin{aligned} C(\tau) &= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^t)-\mathrm{tr}_1^n(\alpha^{d(t+\tau)+l})} \\ &= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^t-\gamma\alpha^{dt})} \\ &= \sum_{x\in\mathbb{F}_{3^n}^*} \omega^{\mathrm{tr}_1^n(x-\gamma x^d)} \end{aligned}$$

where $\gamma = \alpha^{d\tau+l}$ and ω is a primitive third root of unity.

Let $x = y^{3^{n-1}+1}$. Then $x^d = y^{d(3^{n-1}+1)}$. Here we have

$$\begin{aligned} d(3^{n-1}+1) =& \left(\frac{3^n-3^{n/2}+3-1}{3+1}+3^{n/2}\right)(3^{n-1}+1) \\ =& \frac{3^n-3^{n/2}+3-1}{3+1}3^{n-1}+3^{n/2}3^{n-1} \\ &+\frac{3^n-3^{n/2}+3-1}{3+1}+3^{n/2} \end{aligned}$$

$$
\begin{aligned}
&=\frac{3(3^{n-1}+1)-(3^{n/2}+1)}{3+1}3^{n-1}+3^{n+n/2-1}\\
&\quad+\frac{3(3^{n-1}+1)-(3^{n/2}+1)}{3+1}+3^{n/2}\\
&=\frac{3^{n-1}+1}{3+1}-\frac{3^{n/2}+1}{3+1}3^{n-1}+3^{n+n/2-1}\\
&\quad+\frac{3(3^{n-1}+1)}{3+1}-\frac{3^{n/2}+1}{3+1}+3^{n/2}\\
&=\frac{(3+1)(3^{n-1}+1)}{3+1}-\frac{(3^{n/2}+1)(3^{n-1}+1)}{3+1}\\
&\quad+3^{n/2}(3^{n-1}+1)\\
&=3^{n-1}+1+\big(3^{n/2}-\frac{3^{n/2}+1}{3+1}\big)(3^{n-1}+1)\\
&=3^{n-1}+1+\big(\frac{3^{n/2+1}+3^{n/2}-3^{n/2}-1}{3+1}\big)(3^{n-1}+1)\\
&=3^{n-1}+1+\big(\frac{3^{n/2+1}-1}{3+1}\big)(3^{n-1}+1)\\
&=(3^{n-1}+1)\big(\frac{3+1+3^{n/2+1}-1}{3+1}\big)\\
&=(3^{n-1}+1)\big(\frac{3+3^{n/2+1}}{3+1}\big)\\
&=(3^{n-1}+1)\big(\frac{3(3^{n/2+1}+1)}{3+1}\big)\\
&=\frac{3(3^{n-1}+1)}{3+1}(3^{n/2}+1)\\
&=\frac{3^{n}+3}{3+1}(3^{n/2}+1)\\
&=(3^{n}+3)\frac{3^{n/2}+1}{3+1}\\
&=(1+3)\frac{3^{n/2}+1}{3+1}\\
&=3^{n/2}+1 \mod N.
\end{aligned}
$$

Thus, we have

$$\mathrm{tr}_1^n(x-\gamma x^d)=\mathrm{tr}_1^n(y^{3^{n-1}+1}-\gamma y^{3^m+1}).$$

Since $(3^{n-1}+1,3^n-1)=4$, we must consider $a_i\in C_i$, $0\le i\le 3$, so that

$$\begin{aligned}4(1+C(\tau))&=4\left(\sum_{x\in\mathbb{F}_{3^n}}\omega^{\mathrm{tr}_1^n(x-\gamma x^d)}\right)\\&=\sum_{i=0}^{3}\sum_{y\in\mathbb{F}_{3^n}}\omega^{\mathrm{tr}_1^n(a_iy^{3^{n-1}+1}-\gamma a_i^d y^{3^m+1})}\end{aligned}$$

where $C_i=\{\alpha^{4t+i}|0\le t<\frac{3^n-1}{4}\}$.

Here $g_i(y)=\mathrm{tr}_1^n(a_iy^{3^{n-1}+1}-\gamma a_i^d y^{3^m+1})$, $0\le i\le 3$, are quadratic forms. Indeed, let $\{\alpha_k\}$ be a basis of $\mathbb{F}_{3^n}$ over $\mathbb{F}_3$. Then we can set $y=\sum_{k=1}^n y_k\alpha_k$, $y_k\in\mathbb{F}_3$. Thus,

$$\begin{aligned}g_i(y)=&\mathrm{tr}_1^n(a_iy^{3^{n-1}+1}-\gamma a_i^d y^{3^m+1})\\=&\mathrm{tr}_1^n(a_iy^{3^{n-1}+1})-\mathrm{tr}_1^n(\gamma a_i^d y^{3^m+1})\\=&\mathrm{tr}_1^n\Bigg(a_i\Bigg(\sum_{k=1}^n y_k\alpha_k\Bigg)^{3^{n-1}+1}\Bigg)-\mathrm{tr}_1^n\Bigg(\gamma a_i^d\Bigg(\sum_{k=1}^n y_k\alpha_k\Bigg)^{3^m+1}\Bigg)\\=&\mathrm{tr}_1^n\Bigg(a_i\Bigg(\sum_{k=1}^n y_k\alpha_k\Bigg)^{3^{n-1}}\Bigg(\sum_{l=1}^n y_l\alpha_l\Bigg)\Bigg)\\&-\mathrm{tr}_1^n\Bigg(\gamma a_i^d\Bigg(\sum_{k=1}^n y_k\alpha_k\Bigg)^{3^m}\Bigg(\sum_{l=1}^n y_l\alpha_l\Bigg)\Bigg)\\=&\mathrm{tr}_1^n\Bigg(a_i\sum_{k=1}^n y_k\alpha_k^{3^{n-1}}\sum_{l=1}^n y_l\alpha_l\Bigg)-\mathrm{tr}_1^n\Bigg(\gamma a_i^d\sum_{k=1}^n y_k\alpha_k^{3^m}\sum_{l=1}^n y_l\alpha_l\Bigg)\\=&\sum_{k=1}^n\sum_{l=1}^n\mathrm{tr}_1^n(a_iy_ky_l\alpha_k^{3^{n-1}}\alpha_l)-\sum_{k=1}^n\sum_{l=1}^n\mathrm{tr}_1^n(\gamma a_i^d y_ky_l\alpha_k^{3^m}\alpha_l)\end{aligned}$$

$$=\sum_{k=1}^{n}\sum_{l=1}^{n}\mathrm{tr}_1^n(a_i\alpha_k^{3^{n-1}}\alpha_l-\gamma a_i^d\alpha_k^{3^m}\alpha_l)y_ky_l.$$

Therefore, we have the desired exponential sums with quadratic form exponents. In next section, we will restrict the possible rank of quadratic forms.

5.6. Ranks of Quadratic Forms

To calculate possible ranks of quadratic forms, we use Lemma 5.9 and count the number of z such that $g_i(y+z)-g_i(y)=0$ for all $y\in\mathbb{F}_{3^n}$.

Lemma 5.12. The number of z such that $g_i(y+z)-g_i(y)=0$ for all $y\in\mathbb{F}_{3^n}$ equals the number of roots of linearized polynomial $f_i(z)$, where

$$f_i(z)={a_i}^3z^3+a_iz^{3^{n-1}}-(\gamma a_i^d)^{3^m}z^{3^m}-\gamma a_i^dz^{3^m}.$$

Proof. It is easy to verify that

$$\begin{aligned}
&g_i(y+z)-g_i(y)=0\\
\Leftrightarrow\ &\mathrm{tr}_1^n(a_i(y+z)^{3^{n-1}+1}-\gamma a_i^d(y+z)^{3^m+1})-\mathrm{tr}_1^n(a_iy^{3^{n-1}+1}-\gamma a_i^dy^{3^m+1})=0\\
\Leftrightarrow\ &\mathrm{tr}_1^n(y({a_i}^3z^3+a_iz^{3^{n-1}}-(\gamma a_i^d)^{3^m}z^{3^m}-\gamma a_i^dz^{3^m})\\
&+a_iz^{3^{n-1}+1}-\gamma a_i^dz^{3^m+1})=0.
\end{aligned}$$

To satisfy this equation for all y, we must have

$$\begin{aligned}
&{a_i}^3z^3+a_iz^{3^{n-1}}-(\gamma a_i^d)^{3^m}z^{3^m}-\gamma a_iz^{3^m}=0\\
&\mathrm{tr}_1^n(a_iz^{3^{n-1}+1}-\gamma a_i^dz^{3^m+1})=0.
\end{aligned}$$

Note that the first equation is $f_i(z)=0$. Here we claim that the first equation is sufficient condition for the second one. Multiplying the first equation by z, we have

$${a_i}^3z^{3+1}+a_iz^{3^{n-1}+1}-(\gamma a_i^d)^{3^m}z^{3^m+1}-\gamma a_i^dz^{3^m+1}=0.$$

Arranging the equation gives

$$a_i{}^3 z^{3+1} - \gamma a_i^d z^{3^m+1} = -a_i z^{3^{n-1}+1} + (\gamma a_i^d)^{3^m} z^{3^m+1}.$$

Taking the trace function on both sides, we have

$$\mathrm{tr}_1^n(a_i{}^3 z^{3+1} - \gamma a_i^d z^{3^m+1}) = -\mathrm{tr}_1^n(a_i z^{3^{n-1}+1} - (\gamma a_i^d)^{3^m} z^{3^m+1}).$$

Using the property of the trace function, we can raise the first expression of the right-hand side to the third power as

$$\mathrm{tr}_1^n(a_i{}^3 z^{3+1} - \gamma a_i^d z^{3^m+1}) = -\mathrm{tr}_1^n(a_i{}^3 z^{3+1} - \gamma a_i^d z^{3^m+1}).$$

Then we have

$$\begin{aligned}
&\mathrm{tr}_1^n(a_i{}^3 z^{3+1} - \gamma a_i^d z^{3^m+1}) = -\mathrm{tr}_1^n(a_i{}^3 z^{3+1} - \gamma a_i^d z^{3^m+1})\\
&\Leftrightarrow 2\mathrm{tr}_1^n(a_i{}^3 z^{3+1} - \gamma a_i^d z^{3^m+1}) = 0\\
&\Leftrightarrow \mathrm{tr}_1^n(a_i{}^3 z^{3+1} - \gamma a_i^d z^{3^m+1}) = 0.
\end{aligned}$$

□

By the discussion above, it is sufficient to count the number of roots of linearized polynomial $f_i(z)$. Now we prove that the number of roots of the linearized polynomial $f_i(z)$ is one of 1, 9, and 81. Note that the linearized polynomial $f_i(z)$ has the degree 3^{n-1}, which is not constant, but depends on n.

Lemma 5.13. The number of roots of the linearized polynomial $f_i(z)$, $i = 0, 1, 2$ or 3, is one of 1, 9, and 81.

Proof. We can arrange the equation

$$a_i{}^3 z^3 + a_i z^{3^{n-1}} - (\gamma a_i^d)^{3^m} z^{3^m} - \gamma a_i^d z^{3^m} = 0$$

as

$$a_i{}^3 z^3 + a_i z^{3^{n-1}} = ((\gamma a_i^d)^{3^m} + \gamma a_i^d) z^{3^m}.$$

Here we assume $z \neq 0$. By dividing the both sides by z^{3^m}, we obtain

$$\frac{a_i{}^3}{z^{3^m-3}} + a_i z^{3^{n-1}-3^m} = ((\gamma a_i^d)^{3^m} + \gamma a_i^d).$$

Let $X = z^{3^{m-1}-1}$. Since $(3^{m-1}-1, 3^n-1) = 3^2-1 = 8$, this transform is an 8-1 map.

Define

$$B_i = (\gamma a_i^d)^{3^m} + \gamma a_i^d$$
$$Y = a_i X.$$

Then the equality becomes

$$\frac{a_i{}^3}{X^3} + a_i X^{3^m} = B_i.$$

Hence, we have

$$\frac{1}{Y^3} + a_i{}^{3^m+1} Y^{3^m} = B_i.$$

Set $A_i = a_i{}^{3^m+1}$. Note $A_i \in \mathbb{F}_{3^m}$. Let $Y^3 = x$. It is a one-to-one mapping since $(3^n-1, 3) = 1$. Thus,

$$\frac{1}{Y^3} + A_i Y^{3^m} = B_i. \tag{5.1}$$

From (5.1), we have

$$\frac{1}{x} + A_i x^{3^{m-1}} = B_i. \tag{5.2}$$

Now (5.2) can be rewritten as

$$1 + A_i x^{3^{m-1}+1} = B_i x. \tag{5.3}$$

Here we let $x = \frac{1}{B_i} y$. Then (5.3) implies that

$$1 + A_i \left(\frac{1}{B_i} y \right)^{3^{m-1}+1} = B_i \frac{1}{B_i} y. \tag{5.4}$$

(5.4) can be rewritten as

$$1 + \frac{A_i}{B_i^{3^{m-1}+1}} y^{3^{m-1}+1} = y. \tag{5.5}$$

Let $\frac{A_i}{B_i^{3^{m-1}+1}} = \frac{1}{c_i}$. Then (5.5) becomes

$$\begin{aligned} 1 + \frac{1}{c_i} y^{3^{m-1}+1} &= y \\ \Leftrightarrow y^{3^{m-1}+1} - c_i y + c_i &= 0. \end{aligned}$$

Then by Lemma 5.9, the number of solutions of $y^{3^{m-1}+1} - c_i y + c_i = 0$ is one of 0, 1, 2, and $3^{(m-1,n)} + 1 = 3^2 + 1 = 10$. Since the mapping is 8-1 map, the number of solutions is one among 0, 8, 16, and 80. Adding a zero root ($z = 0$), we have 1, 9, 17, and 81. Since the original equation is a linearized polynomial, 17 cannot be a number of root. Thus the linearized polynomial can have only 1, 9, or 81 roots. □

Next we show that among the four linearized polynomials $f_i(z)$, $0 \leq i \leq 3$, at most one polynomial can have 81 roots.

Lemma 5.14. Among the four linearized polynomials $f_i(z)$, $0 \leq i \leq 3$, at most one polynomial can have 81 solutions. Or equivalently, among four polynomials $h_i(y) = y^{3^{m-1}+1} - c_i y + c_i$, $0 \leq i \leq 3$, at most one polynomial can have 10 solutions.

Proof. Without loss of generality, we may assume that $a_i = \alpha^i$. By the previous lemma, we have the following relation

$$c_i = \frac{(\mathrm{tr}_m^n(\gamma a_i^d))^{3^{m-1}+1}}{a_i^{3^m+1}}, \quad y = \frac{\mathrm{tr}_m^n(\gamma a_i^d)}{a_i^3} z^{3^m-3}. \tag{5.6}$$

Suppose $\beta = \alpha^{\frac{3^n-1}{3^m-1}} = \alpha^{3^m+1}$ is a primitive element of the subfield $\mathbb{F}_{3^m}$. Since

$$a_i^{3^m+1} = (\alpha^i)^{3^m+1} = \beta^i,$$

for $i = 0, 2$, $a_i^{3^m+1}$ is a square in the subfield and for $i = 1, 3$, $a_i^{3^m+1}$ is a nonsquare element of the subfield. Note that the numerator $(\mathrm{tr}_m^n(\gamma a_i^d))^{3^{m-1}+1}$ is always a square in the subfield $\mathbb{F}_{3^m}$. Consequently,

$$c_i = \begin{cases} \text{square in } \mathbb{F}_{3^m} & \text{if } i = 0, 2 \\ \text{nonsquare in } \mathbb{F}_{3^m} & \text{if } i = 1, 3. \end{cases}$$

Now we claim that only $f_0(z)$ can have 81 roots. Suppose $f_i(z)$ has 81 roots. We consider the following two cases.

Case 1) $i = 0$ or $i = 2$:

By Corollary 5.11, we have

$$\left(\frac{y^{3^{m-1}+1}}{c_i}\right)^{\frac{3^n-1}{3^2-1}} = (y-1)^{\frac{3^n-1}{3^2-1}} = 1. \tag{5.7}$$

Since c_i is a square in $\mathbb{F}_{3^m}$, $c_i = \beta^{2k}$ for some k. Also note that $\beta = \alpha^{4l}$ for some l. Therefore we have

$$c_i^{\frac{3^n-1}{3^2-1}} = (\alpha^{8kl})^{\frac{3^n-1}{3^2-1}} = 1.$$

Thus $(y^{3^{m-1}+1})^{\frac{3^n-1}{3^2-1}} = 1$. Since $3^{m-1} + 1 = 2 \bmod 4$, we can substitute as $y^{3^{m-1}+1} = x^{4k+2}$. Then we have

$$(x^{4k+2})^{\frac{3^n-1}{8}} = (x^{2k+1})^{\frac{3^n-1}{4}} = 1.$$

Therefore,

$$y^{\frac{3^{m-1}+1}{2}} = x^{2k+1} = \alpha^{4l'} \text{ for some } l'.$$

But since $(\frac{3^{m-1}+1}{2}, 4) = 1$, we have $y = \alpha^{4l'}$. Thus, from (5.6),

$$ya_i^3 = \mathrm{tr}_m^n(\gamma a_i^d) z^{3^m-3}.$$

Here all terms in the right hand side are in C_0. We already observed that $y \in C_0$. Therefore we must have $a_i \in C_0$. This implies that $i = 0$.

Case 2) $i = 1$ or $i = 3$:

Now assume that $i = 1$ or $i = 3$. This means that c_i is a nonsquare in $\mathbb{F}_{3^n}$. Thus, we can write

$$c_i = \beta^{2k+1} = (\alpha^{4l})^{2k+1} = \alpha^{8lk+4l}.$$

Note that l is odd since m is odd. Applying Corollary 5.11 again, we have (5.7), but for this case, it follows that

$$c_i^{\frac{3^n-1}{3^2-1}} = (\alpha^{2lk+l})^{\frac{3^n-1}{2}} = (-1)^{(2k+1)l} = -1.$$

Therefore

$$(y^{3^{m-1}+1})^{\frac{3^n-1}{3^2-1}} = -1.$$

Since $3^{m-1}+1 = 2 \bmod 4$, we can substitute as $3^{m-1}+1 = 4k+2$ for some k. Then we have

$$(y^{2k+1})^{\frac{3^n-1}{4}} = -1 \Leftrightarrow \left(y^{\frac{3^n-1}{2}}\right)^k y^{\frac{3^n-1}{4}} = \alpha^{\frac{3^n-1}{2}k'} \tag{5.8}$$

where k' is some odd integer. Thus y must be a square in $\mathbb{F}_{3^n}$. Let $y = \alpha^{2l'}$ for some integer l'. From (5.8), it follows that

$$\alpha^{\frac{3^n-1}{2}l'} = \alpha^{\frac{3^n-1}{2}k'}.$$

Therefore, l' is odd. Thus $y \in C_2$. From (5.6), we have $a_i \in C_2$. This implies that c_i is in C_2, which contradicts $i = 1$ or $i = 3$. Therefore if $f_i(z)$ has 81 roots, then $i = 0$. □

It is well known that the number of roots of the linearized polynomial

$f_i(z)$ is equal to $3^{n-\mathrm{rank}(g_i(y))}$. Therefore by what we have discussed so far, each $g_i(y)$ has a rank of n, $n-2$, or $n-4$, and only one of $g_i(y)$, $i=0,1,2,3$, can have the rank $n-4$. Thus we can enumerate 9 possible rank combinations of $g_i(y)$, $i=0,1,2,3$, ignoring order as

$$\begin{aligned}&(n,n,n,n),\ (n,n,n,n-2),\ (n,n,n,n-4),\\&(n,n,n-2,n-2),\ (n,n,n-2,n-4),\\&(n,n-2,n-2,n-2),\ (n,n-2,n-2,n-4),\\&(n-2,n-2,n-2,n-2),\ (n-2,n-2,n-2,n-4).\end{aligned}\tag{5.9}$$

5.7. Upper Bound on the Cross-Correlation Function

Now we are ready to derive the upper bound on the magnitude of the cross-correlation function. This can be done by applying Lemma 5.6 and Lemma 5.7 to each of rank combinations of $g_i(y)$, $i=0,1,2,3$.

Theorem 5.15. For an integer $k \geq 0$, $n=4k+2=2m$, $d=\frac{3^n-3^m+2}{4}+3^m$, and $0 \leq l < 4(3^m+1)$, the magnitude of the cross-correlation function $C(\tau)$ between $\mathrm{tr}_1^n(\alpha^t)$ and $\mathrm{tr}_1^n(\alpha^{dt+l})$ is upper bounded by

$$|C(\tau)| \leq 4.5 \cdot 3^m + 1.$$

Proof. As discussed before, there are nine rank combinations for $g_i(y)$, $i=0,1,2,3$, ignoring ordering. We bound the magnitude of the cross-correlation for each case.

Case 1) The rank combination is given as (n,n,n,n);

We have

$$\begin{aligned}4(1+C(\tau)) &= \sum_{i=0}^{3}\sum_{y\in\mathbb{F}_{3^n}}\omega^{g_i(y)}\\ &= \epsilon_1 3^{\frac{n}{2}} + \epsilon_2 3^{\frac{n}{2}} + \epsilon_3 3^{\frac{n}{2}} + \epsilon_4 3^{\frac{n}{2}}\\ &= (\epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4)3^m\\ &\leq 4\cdot 3^m\end{aligned}$$

where $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 = \pm 1$. Thus, we obtain $|C(\tau)| \leq 3^m + 1$.

Case 2) The rank combination is given as $(n, n, n, n-2)$;

We have

$$\begin{aligned}4(1+C(\tau)) &= \sum_{i=0}^{3}\sum_{y\in\mathbb{F}_{3^n}}\omega^{g_i(y)}\\ &= \epsilon_1 3^{\frac{n}{2}} + \epsilon_2 3^{\frac{n}{2}} + \epsilon_3 3^{\frac{n}{2}} + \epsilon_4 3^2 3^{\frac{n-2}{2}}\\ &= (\epsilon_1+\epsilon_2+\epsilon_3)3^m + 3\epsilon_4 3^m\\ &\leq 6\cdot 3^m\end{aligned}$$

where $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 = \pm 1$. Thus, we obtain $|C(\tau)| \leq \frac{3}{2}3^m + 1$.

Case 3) The rank combination is given as $(n, n, n, n-4)$;

We have

$$\begin{aligned}4(1+C(\tau)) &= \sum_{i=0}^{3}\sum_{y\in\mathbb{F}_{3^n}}\omega^{g_i(y)}\\ &= \epsilon_1 3^{\frac{n}{2}} + \epsilon_2 3^{\frac{n}{2}} + \epsilon_3 3^{\frac{n}{2}} + \epsilon_4 3^4 3^{\frac{n-4}{2}}\\ &= (\epsilon_1+\epsilon_2+\epsilon_3)3^m + 3^2\epsilon_4 3^m\\ &\leq 12\cdot 3^m\end{aligned}$$

where $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 = \pm 1$. Thus, we obtain $|C(\tau)| \leq 3\cdot 3^m + 1$.

Case 4) The rank combination is given as $(n, n, n-2, n-2)$;

We have

$$\begin{aligned}
4(1+C(\tau)) &= \sum_{i=0}^{3} \sum_{y\in\mathbb{F}_{3^n}} \omega^{g_i(y)} \\
&= \epsilon_1 3^{\frac{n}{2}} + \epsilon_2 3^{\frac{n}{2}} + \epsilon_3 3^2 3^{\frac{n-2}{2}} + \epsilon_4 3^2 3^{\frac{n-2}{2}} \\
&= (\epsilon_1+\epsilon_2)3^m + 3\epsilon_4 3^m + 3\epsilon_4 3^m \\
&\le 8\cdot 3^m
\end{aligned}$$

where $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 = \pm 1$. Thus, we obtain $|C(\tau)| \le 2\cdot 3^m + 1$.

Case 5) The rank combination is given as $(n, n, n-2, n-4)$;

We have

$$\begin{aligned}
4(1+C(\tau)) &= \sum_{i=0}^{3} \sum_{y\in\mathbb{F}_{3^n}} \omega^{g_i(y)} \\
&= \epsilon_1 3^{\frac{n}{2}} + \epsilon_2 3^{\frac{n}{2}} + \epsilon_3 3^2 3^{\frac{n-2}{2}} + \epsilon_4 3^4 3^{\frac{n-4}{2}} \\
&= (\epsilon_1+\epsilon_2)3^m + 3\epsilon_3 3^m + 3^2\epsilon_4 3^m \\
&\le 14\cdot 3^m
\end{aligned}$$

where $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 = \pm 1$. Thus, we obtain $|C(\tau)| \le \frac{7}{2}\cdot 3^m + 1$.

Case 6) The rank combination is given as $(n, n-2, n-2, n-2)$;

We have

$$\begin{aligned}
4(1+C(\tau)) &= \sum_{i=0}^{3} \sum_{y\in\mathbb{F}_{3^n}} \omega^{g_i(y)} \\
&= \epsilon_1 3^{\frac{n}{2}} + \epsilon_2 3^2 3^{\frac{n-2}{2}} + \epsilon_3 3^2 3^{\frac{n-2}{2}} + \epsilon_4 3^2 3^{\frac{n-2}{2}} \\
&= \epsilon_1 3^m + 3\epsilon_2 3^m + 3\epsilon_4 3^m + 3\epsilon_4 3^m \\
&\le 13\cdot 3^m
\end{aligned}$$

where $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 = \pm 1$. Thus, we obtain $|C(\tau)| \le \frac{13}{4}\cdot 3^m + 1$.

Case 7) The rank combination is given as $(n, n-2, n-2, n-4)$;

We have

$$\begin{aligned}
4(1+C(\tau)) &= \sum_{i=0}^{3} \sum_{y \in \mathbb{F}_{3^n}} \omega^{g_i(y)} \\
&= \epsilon_1 3^{\frac{n}{2}} + \epsilon_2 3^2 3^{\frac{n-2}{2}} + \epsilon_3 3^2 3^{\frac{n-2}{2}} + \epsilon_4 3^4 3^{\frac{n-4}{2}} \\
&= \epsilon_1 3^m + 3\epsilon_2 3^m + 3\epsilon_3 3^m + 3^2 \epsilon_4 3^m \\
&\leq 16 \cdot 3^m
\end{aligned}$$

where $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 = \pm 1$. Thus, we obtain $|C(\tau)| \leq 4 \cdot 3^m + 1$.

Case 8) The rank combination is given as $(n-2, n-2, n-2, n-2)$;

We have

$$\begin{aligned}
4(1+C(\tau)) &= \sum_{i=0}^{3} \sum_{y \in \mathbb{F}_{3^n}} \omega^{g_i(y)} \\
&= \epsilon_1 3^2 3^{\frac{n-2}{2}} + \epsilon_2 3^2 3^{\frac{n-2}{2}} + \epsilon_3 3^2 3^{\frac{n-2}{2}} + \epsilon_4 3^2 3^{\frac{n-2}{2}} \\
&= 3\epsilon_1 3^m + 3\epsilon_2 3^m + 3\epsilon_4 3^m + 3\epsilon_4 3^m \\
&\leq 12 \cdot 3^m
\end{aligned}$$

where $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 = \pm 1$. Thus, we obtain $|C(\tau)| \leq 3 \cdot 3^m + 1$.

Case 9) The rank combination is given as $(n-2, n-2, n-2, n-4)$;

We have

$$\begin{aligned}
4(1+C(\tau)) &= \sum_{i=0}^{3} \sum_{y \in \mathbb{F}_{3^n}} \omega^{g_i(y)} \\
&= \epsilon_1 3^2 3^{\frac{n-2}{2}} + \epsilon_2 3^2 3^{\frac{n-2}{2}} + \epsilon_3 3^2 3^{\frac{n-2}{2}} + \epsilon_4 3^4 3^{\frac{n-4}{2}} \\
&= 3\epsilon_1 3^m + 3\epsilon_2 3^m + 3\epsilon_3 3^m + 3^2 \epsilon_4 3^m \\
&\leq 18 \cdot 3^m
\end{aligned}$$

where $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 = \pm 1$. Thus, we obtain $|C(\tau)| \leq 4.5 \cdot 3^m + 1$.

Hence the magnitude of the cross-correlation function $C(\tau)$ is upper bounded by $|C(\tau)| \leq 4.5 \cdot 3^m + 1$. □

5.8. Examples

In this section, we consider examples of cross-correlations studied in the previous sections.

Example 5.16. Suppose $n = 4k+2 = 2m = 6$ and $d = 203$. For all l going through 0 to $\frac{3^m+1}{4} - 1 = 103$, by computer search, the cross-correlation distribution between $\mathrm{tr}_1^n(\alpha^t)$ and $\mathrm{tr}_1^n(\alpha^{dt+l})$ is given as

$$C(\tau) = \begin{cases} -1, & 34328 \text{ times} \\ -28, & 18095 \text{ times} \\ 26, & 14973 \text{ times} \\ -82, & 833 \text{ times} \\ 80, & 938 \text{ times} \\ -55, & 4676 \text{ times} \\ 53 & 1869 \text{ times.} \end{cases}$$

Note that the cross-correlation is 7-valued. The maximum magnitude of correlation is $82 \approx 3.039\sqrt{3^6 - 1}$.

Example 5.17. Let $m = 5$, $n = 10$. Then $d = 14945$. By the computer experiments, the cross-correlation is given as

$$C(\tau) = \begin{cases} 728, & 21411 \text{ times} \\ -487, & 64050 \text{ times} \\ -1, & 1473577 \text{ times} \\ 485, & 206180 \text{ times} \\ -244, & 963190 \text{ times} \\ 242, & 812520 \text{ times} \\ -730 & 61000 \text{ times.} \end{cases}$$

The cross-correlation is again 7-valued. The maximum magnitude of correlation is $730 \approx 3.004\sqrt{3^{10} - 1}$.

5.9. Related Works

After [59] was presented, Xia, Chen, Helleseth, and Li [49] generalized the result to the odd prime p case. To be specific, for an odd positive integer $m \geq 3$, $n = 2m$, and an odd prime p, they derived the cross-correlation between the p-ary m-sequence $\mathrm{tr}_1^n(\alpha^t)$ and its all decimated sequences $\mathrm{tr}_1^n(\alpha^{dt+l})$ for the decimation factor $d = \frac{(p^m+1)(p^m+p-1)}{p+1}$, where $0 \leq l < \gcd(d, p^n - 1)$ and α is a primitive element of $\mathbb{F}_{p^n}$. They showed that the cross-correlation function takes values in $\{-1, -1 \pm ip^m | i = 1, 2, ..., p\}$.

Theorem 5.18 (Xia, Chen, Helleseth, and Li [49])**.** Let p be an odd prime, $m \geq 3$ be an odd integer, and $n = 2m$. Let $d = \frac{(p^m+1)(p^m+p-1)}{p+1}$ be the decimation factor. Then the cross-correlation function between $\mathrm{tr}_1^n(\alpha^t)$ and its all decimated sequences $\mathrm{tr}_1^n(\alpha^{dt+l})$, where $0 \leq l < \gcd(d, p^n - 1)$, takes the values belonging to the following set

$$\{-1, -1 \pm ip^m | i = 1, 2, ..., p\}.$$

Therefore, the magnitude of the cross-correlation is upper bounded by $p^{m+1} + 1$. □

Note that our result is the special case for $p = 3$.

5.10. Conclusion

In this chapter, we investigate the upper bound on the cross-correlation function between a ternary m-sequence of period $3^n - 1$, $n = 4k + 2$ and its decimated sequence with the decimation $d = \frac{3^{4k+2} - 3^{2k+1} + 2}{4} + 3^{2k+1}$. It is shown that the cross-correlation is upper bounded by $4.5 \cdot 3^{n/2} + 1$. For the derivation, it is proved that 1, 9, 81 are only possible number of solutions of linearized polynomials and only one among four linearized polynomials can have 81 roots. This result is further improved by Xia, Chen, Helleseth, and Li [49].

Chapter 6. Conclusions

In this dissertation, we construct half-period sequence families with low correlation using the shift-and-add method and the decimation. We consider p-ary sequences for sequence family constructions and give an upper bound on the correlation within the sequence families.

In the second part of this dissertation, we consider the Helleseth's work [11] and derive the cross-correlation values of decimated m-sequences.

The last topic of this dissertation is the derivation of the upper bound on the cross-correlation between ternary m-sequences and its decimations with the particular decimation factor. Proving the upper bound requires the quadratic form technique and Bluher's result [33].

In Chapter 2, pseudorandom sequences have been introduced. Some well known sequences and sequence families are reviewed, and necessary definitions and mathematical preliminaries are explained.

In Chapter 3, new families of half-period p-ary sequences with low correlation are proposed. For an odd prime $p = 3 \mod 4$ and an odd positive integer n, families of sequences of period $N = \frac{p^n-1}{2}$ are constructed from m-sequences and their decimated sequences by $d = N - p^{n-1}$. Using the generalized Kloosterman sums, we show that the upper bound on the correlation of the family is $2\sqrt{N + \frac{1}{2}}$, which is about 1.5 times of the Sidel'nikov's lower bound. The family size is given as $4N$.

In Chapter 4, we study the values of the cross-correlation of two decimated m-sequences. We consider two p-ary m-sequences with the period of $p^n - 1$ for an odd prime p and an even integer n, decimated each by 2 and $4p^{n/2} - 2$, respectively. Our study is based on the Helleseth's work [11] and consequently the correlation function takes only values in $\left\{ \frac{-1 \pm p^{n/2}}{2}, \frac{-1+3p^{n/2}}{2}, \frac{-1+5p^{n/2}}{2} \right\}$. Furthermore, for $p^{n/2} \neq 2 \mod 3$, we propose half-period sequence families which have the maximum correlation magnitude $\frac{-1+5p^{n/2}}{2}$. The size of the family is given as $2(p^n - 1)$.

In Chapter 5, for $n = 4k + 2$, the cross-correlation between ternary m-sequences and decimated m-sequences by the decimation factor $d = \frac{3^{4k+2} - 3^{2k+1} + 3 - 1}{3+1} + 3^{2k+1}$ is investigated. We employ the quadratic form technique and Bluher's result [33] for the derivation of the upper bound on the correlation. It is proved that the upper bound is given by $4.5 \cdot 3^{n/2} + 1$.

Bibliography

[1] N. Zierler, "Legendre sequences," Group Report 34-71, Lincoln Lab., M. I. T., Lexington, May, 1958.

[2] T. Kasami, "Weight distribution formular for some class of cyclic codes," Technical Report R-285 (AD 632574), Coordinated Science Laboratory, Univ. of Illinois, Urbana, Apr. 1966.

[3] T. Kasami, "Weight distribution of Bose-Chaudhuri-Hocquenghem codes," in *Cambinatorial Mathematics and Its Applications.* Chapel Hill, NC: Univ. of North Carolina Press, 1969.

[4] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inf. Theory*, pp. 154-156, Jan. 1968.

[5] V. M. Sidelnikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," *Prbl. Inf. Transm.*, vol. 5, no. 1, pp. 12-16, May. 1969.

[6] V. M. Sidelnikov, "On mutual correlation of sequences," *Soviet Math. Dokl.*, vol. 12, no. 1, pp. 197-201, 1971.

[7] H. M. Trachtenberg, "On the cross-correlation functions of maximal recurring sequences," Ph.D. dissertation, Univ. of Southern California, Los Angeles, CA, 1970.

[8] Y. Niho, "Multi-valued cross-correlation functions between two maximal recursive sequences," Ph.D. dissertation, Univ. of Southern California, Los Angeles, CA, 1972.

[9] L. D. Baumert and R. J. McEliece, "Weight of irreducible cyclic codes," *Information and Control*, vol. 20, no. 2, Mar. 1972.

[10] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 397-399, May 1974.

[11] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discr. Math.*, vol. 16, pp. 209-232, 1976.

[12] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation function," *IEEE Trans. Inf. Theory*, vol. 48, pp. 2868-2872, 2002.

[13] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inf. Theory*, vol. 28, no. 6, pp. 858-864, Nov. 1982.

[14] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inf. Theory*, vol. 30, no. 3, pp. 548-553, May 1984.

[15] J. S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal correlation properties and large linear span," *IEEE Trans. Inf. Theory*, vol. 35, no. 2, pp. 371-379, Mar. 1989.

[16] J. S. No, "Generalization of GMW and No sequences," *IEEE Trans. Inf. Theory*, vol. 42, no. 1, pp. 260-262, Jan. 1996.

[17] J. S. No, H. Chung, Y. Yang, and H. Y. Song, "New construction for families of binary sequences with optimal correlation properties," *IEEE Trans. Inf. Theory*, vol. 43, no. 5, pp. 1596-1602, Sep. 1997.

[18] J. S. No, S. W. Golomb, G. Gong, H. K. Lee, and P. Gaal, "Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 814-817, Mar. 1998.

[19] J. S. No, H. Chung, and M. S. Yun, "Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 2060-2065, Sep. 1999.

[20] J. S. No, H. Chung, H. Y. Song, K. Yang, J. D. Lee, and T. Helleseth, "New construction for binary sequences of period $p^m - 1$ with optimal autocorrelation using $(z+1)^d + az^d + b$," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1638-1644, May 2001.

[21] J. S. No, "p-ary unified sequences: p-ary extended d-form sequences with ideal autocorrelation property," *IEEE Trans. Inf. Theory*, vol. 48, pp. 2540-2546, Sep. 2002.

[22] J. S. No, G. M. Gil, and D. J. Shin, "Generalized construction of binary bent sequences with optimal correlation property," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1769-1780, Jul. 2003.

[23] P. V. Kumar and O. Moreno, “Prime-phase sequences with periodic correlation properties better than binary sequences,” *IEEE Trans. Inf. Theory*, vol. 37, pp. 603-616, May 1991.

[24] S. C. Liu and J. F. Komo, “Nonbinary Kasami sequences over $GF(p)$,” *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1409-1412, Jul. 1992.

[25] A. Lin, “From cyclic Hadamard difference sets to perfectly balanced sequences,” Ph.D. dissertation, Univ. of Southern California, Los Angeles, CA, 1998.

[26] V. I. Levenshtein, “New lower bounds on aperiodic crosscorrelation of binary codes,” *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 284-288, Jan. 1999.

[27] E. N. Muller, “On the cross-correlation of sequences over GF(p) with short periods,” *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 289-295, Jan. 1999.

[28] Z. Hu, X. Li, D. Mills, E. N. Muller, W. Sun, W. Willems, Y. Yang, and Z. Zhang, “On the crosscorrelation of sequences with the decimation factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$,” *Appl. Algebra Eng. Commun. Comput.*, vol. 12, no. 3, pp. 255-263, 2001.

[29] H. Dobbertin, T. Helleseth, P. V. Kumar, and H. Martinsen, “Ternary m-sequences with three-valued cross-correlation function: New decimations of Welch and Niho type,” *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1473-1481, May 2001.

[30] Y. S. Kim, J. W. Jang, J. S. No, and T. Helleseth, “New constructions of p-ary bent sequences,” *IEICE Trans. Fund. Electron., Commun. Comp. Sci.*, vol. E87-A, no.2, pp. 489-494, Feb. 2004.

[31] Y. S. Kim, J. S. Chung, J. S. No, and H. Chung, “New families of M-ary sequences with low correlation constructed from Sidel’nikov sequences,” *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3768-3774, Aug. 2008.

[32] J. W. Jang, Y. S. Kim, J. S. No, and T. Helleseth, “New families of p-ary sequences with optimal correlation property and large linear span,” *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1839-1844, Aug. 2004.

[33] A. W. Bluher, “On $x^{q+1} + ax + b$,” *Finite Fields and Their Applications*, vol. 10, no. 3, pp. 285-305, Jul. 2004.

[34] G. J. Ness, T. Helleseth, and A. Kholosha, “On the correlation distribution of the Coulter-Matthews decimation,” *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2241-2247, May 2006.

[35] X. Zeng, N. Li, and L. Hu, “A class of nonbinary codes and sequence families,” *Sequences and Their Applications 2008*, Sep. 14-18, 2008.

[36] E. Y. Seo, Y. S. Kim, J. S. No, and D. J. Shin, “Cross-correlation distribution of p-ary m-sequence and its $p + 1$ decimated sequence with shorter period,” *IEICE Trans. Fund. Electron., Commun. Comp. Sci.*, vol. E90-A, no.11, pp. 2568-2574, Nov. 2007.

[37] E. Y. Seo, Y. S. Kim, J. S. No, and D. J. Shin, "Cross-correlation distribution of p-ary m-sequence of period $p^{4k}-1$ and its decimated sequences by $\left(\frac{p^{2k}+1}{2}\right)^2$," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3140-3149, Jul. 2008.

[38] Y. K. Han and K. Yang, "New M-ary sequence families with low correlation and large size," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1815-1823, Apr. 2009.

[39] N. Y. Yu and G. Gong, "New construction of M-ary sequence families with low correlation from the structure of Sidelnikov sequences," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 4061-4070, Aug. 2010.

[40] N. Y. Yu and G. Gong, "Multiplicative characters, the Weil bound, and polyphase sequence families with low correlation," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6376-6387, Dec. 2010.

[41] K. T. Arasu, J. F. Dillon, and K. J. Player, "Character sum factorizations yield perfect sequences," preprint, 2010.

[42] J. Luo, "Cross correlation of nonbinary Niho-type sequences," *IEEE International Symposium on Information Theory*, pp.1297-1299, Austin, TX, Jun. 2010.

[43] J. Luo, T. Helleseth, and A. Kholosha, "Two nonbinary sequences with six-valued cross-correlation," *Proc. Fifth International Workshop on Signal Design and its Applications in Communications*, pp.44-47, Guilin, Oct. 2011.

[44] K-U. Schmidt, “Sequence families with low correlation derived from multiplicative and additive characters,” *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2291-2294, Apr. 2011.

[45] J. S. Chung, J. S. No, and H. Chung, “A construction of a new family of M-ary sequences with low correlation from Sidel’nikov sequences,” *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2301-2305, Apr. 2011.

[46] Y. Xia, X. Zeng, and Li. Hu, “Further crosscorrelation properties of sequences with the decimation factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$,” *Appl. Algebra Eng. Commun. Comput.*, vol. 21, no. 5, pp. 329-342, 2010.

[47] Y. Xia and S. Chen, “A new family of p-ary sequences with low correlation constructed from decimated sequences,” *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 6037-6046, Sep. 2012.

[48] Y. Xia and S. Chen, “Cross-correlation distribution between a p-ary m-sequence and its decimated sequence with decimation factor $d = \frac{(p^m+1)^2}{2(p^e+1)}$,” *IEICE Trans. Fund. Electron., Commun. Comp. Sci.*, vol. E97-A, no. 4, pp. 964-969, Apr. 2014.

[49] Y. Xia, S. Chen, T. Helleseth, and C. Li, “Cross-correlation between a p-ary m-sequence and its all decimated sequences for $d = \frac{(p^m+1)(p^m+p-1)}{(p+1)}$,” *IEICE Trans. Fund. Electron., Commun. Comp. Sci.*, vol. E97-A, no. 4, pp. 964-969, Apr. 2014.

[50] S. T. Choi, J. S. No, and H. Chung, “On the cross-correlation of a ternary m-sequence of period $3^{4k+2}-1$ and its decimated sequence by

$\frac{(3^{2k+1}+1)^2}{8}$," *IEEE International Symposium on Information Theory*, pp. 1268-1271, Austin, TX, Jun. 2010.

[51] S. T. Choi, T. H. Lim, J. S. No, and H. Chung, "Evaluation of cross-correlation values of p-ary m-sequence and its decimated sequence by $\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$," *IEEE International Symposium on Information Theory*, pp. 637-641, St. Petersburg, Russia, Jul. 2011.

[52] S. T. Choi, T. H. Lim, J. S. No, and H. Chung, "On the cross-correlation of a p-ary m-sequence of period $p^{2m}-1$ and its decimated sequences by $\frac{(p^m+1)^2}{2(p+1)}$," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1873-1879, Mar. 2012.

[53] S. T. Choi, J. Y. Kim, J. S. No, and H. Chung, "Weight distribution of some cyclic codes," *IEEE International Symposium on Information Theory*, pp. 2911-2913, Cambridge, MA, Jul. 2012.

[54] S. T. Choi and J. S. No, "On the cross-correlation distributions of p-ary m-sequences and their decimated sequences," *IEICE Trans. Fund. Electron., Commun. Comp. Sci.*, vol. E95-A, no. 11, pp. 1808-1818, Nov. 2012.

[55] S. T. Choi, J. Y. Kim, and J. S. No, "On the cross-correlation of a p-ary m-sequence and its decimated sequences by $d=\frac{p^n+1}{p^k+1}+\frac{p^n-1}{2}$," *IEICE Transactions on Communications*, vol. E96-B, no. 9, pp. 2190-2197, Sep. 2013.

[56] Y. Sun, Z. Wang, H. Li, and T. Yan, "The cross-correlation distribution of a p-ary m-sequence of period $p^{2k}-1$ and its decimated sequence by $\frac{(p^k+1)^2}{2(p^e+1)}$," *Advances in Mathematics of Communications*, vol. 7, no. 4, pp. 409-424 , Nov. 2013.

[57] J. Y. Kim, S. T. Choi, T. H. Lim, J. S. No, and H. Chung, "A new family of p-ary decimated sequences with low correlation," *IEEE International Symposium on Information Theory*, pp. 1264-1267, Austin, TX, Jun. 2010.

[58] J. Y. Kim, S. T. Choi, and J. S. No, "A new family of p-ary sequences of period $(p^n-1)/2$ with low correlation," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3825-3829, Jun. 2011.

[59] J. Y. Kim, S. T. Choi, T. H. Lim, J. S. No, and H. Chung, "On the cross-correlation of ternary m-sequences of period $3^{4k+2}-1$ with decimation $\frac{3^{4k+2}-3^{2k+1}+2}{4}+3^{2k+1}$," *IEEE International Symposium on Information Theory*, pp. 1019-1023, Cambridge, MA, Jul. 2012.

[60] J. Y. Kim, C. M. Cho, W. J. Lee, and J. S. No, "On the cross-correlation between two decimated p-ary m-sequences by 2 and $4p^{n/2}-2$," to appear in *IEICE Transactions on Communications*, vol. E98-B, no. 3, Mar. 2015.

[61] D. S. Kim, H. J. Chae, and H. Y. Song, "A generalization of the family of p-ary decimated sequences with low correlation," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7614-7617, Nov. 2011.

[62] W. J. Lee, J. Y. Kim, and J. S. No, “New families of p-ary sequences of period $(p^n - 1)/2$ with low maximum correlation magnitude,” *IEICE Transactions on Communications*, vol. E97-B, no. 11, pp. 2311-2315, Nov. 2014.

[63] C. M. Cho, J. Y. Kim, and J. S. No, “New p-ary sequence families of period $\frac{p^n-1}{2}$ with good correlation property using two decimated m-sequences,” submitted to *IEEE Trans. Inf. Theory*, May 2014.

[64] C. M. Cho, J. Y. Kim, and J. S. No, “Cross-correlation distribution between two decimated sequences by 2 and $\frac{(p^m+1)^2}{2}$,” *IEEE International Symposium on Information Theory*, pp. 1653-1657, Honolulu, HI, Jun. 2014.

[65] H. Hu, S. Shao, G. Gong, and T. Helleseth, “The proof of Lin’s conjecture via the decimation-Hadamard transform,” *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 5054-5064, Aug. 2014.

[66] L. E. Dickson, *Linear Groups With An Exposition of The Galois Field Theory.* New York, NY: Dover Publications, 1958.

[67] T. Storer, *Cyclotomy and Difference Sets, Lectures in Advanced Mathematics.* Chicago, IL: Markham, 1967.

[68] E. R. Berlekamp, *Algebraic Coding Theory.* New York, NY: McGraw-Hill, 1968.

[69] S. W. Golomb, *Shift-Register Sequences.* Laguna Hills, CA: Aegean Park Press, 1981.

[70] R.Lidl and H.Niederreliter, *Finite Fields, vol.20, Encyclopedia of Mathematics and its Applications.* Amsterdam, The Netherlands: Addison-Wesley, 1983.

[71] T. Helleseth and P. V. Kumar, “Sequences with low correlation,” in *Handbook of Coding Theory*, ed. V. Pless and C. Huffman, Amsterdam, The Netherlands: Elsevier Science, 1998.

[72] S. Lang, *Algebra.* New York, NY: Springer, 2002.

[73] 이인석, 학부 대수학 강의 I - 선형대수와 군, 서울대학교출판부, 2005.

[74] S. W. Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communication, Cryptography, and Radar.* New York, NY: Cambridge University Press, 2005.

[75] A. Goldsmith, *Wireless Communications.* Singapore, Singapore: Cambridge University Press, 2005.

[76] C. Paar and J. Pelzl, *Understanding Cryptography.* Berlin Heidelberg, Germany: Springer, 2010.

[77] M. Goresky and A. Klapper, *Algebraic Shift Register Sequences.* New York, NY: Cambridge University Press, 2012.

초 록

본 논문은 세 가지의 연구 결과를 포함하고 있다. 주기 $\frac{p^n-1}{2}$를 가지는 새로운 p진 수열군의 생성, 데시메이션된 p진 m-수열과 그 데시메이션 사이의 상호상관도에 대한 연구, 마지막으로 3진 m-수열과 그 데시메이션 수열 사이의 상호상관도에 관한 연구이다.

먼저, $p = 3 \mod 4$를 만족하는 홀수인 소수 p와 홀수 n에 대해서, 낮은 상관도를 가지는 주기 $N = \frac{p^n-1}{2}$의 새로운 p진 수열 군을 제안하였다. 본 수열군은 두 개의 데시메이션된 m-수열을 이용하였으며, 이 때 데시메이션의 값은 각각 2와 $d = N - p^{n-1}$으로 주어진다. 상호상관도의 절대값의 상한은 $2\sqrt{N + 1/2} = \sqrt{2p^n}$으로 주어지며 이는 일반화된 클루스터만 합에 의해 유도된다. 수열군의 크기는 주기의 네 배로서, $2(p^n - 1)$으로 주어진다.

두 번째 결과로, Helleseth [11]의 결과로부터, 홀수 소수인 p와 정수 $n = 2m$에 대해 각각 2와 $4p^{n/2} - 2$로 데시메이션된 두 개의 p진 m-수열간의 상호상관도가 분석되었다. 상호상관도는 최대 4개의 값을 가질 수 있으며, 이는 $\frac{-1 \pm p^{n/2}}{2}, \frac{-1+3p^{n/2}}{2}, \frac{-1+5p^{n/2}}{2}$ 중의 하나이다. 본 결과를 이용하여 $p^m \neq 2 \mod 3$인 경우에 대해서, 상호상관도의 크기가 $\frac{5}{\sqrt{2}}\sqrt{N}$이고 주기가 $N = \frac{p^n-1}{2}$, 수열군의 크기 $4N$를 가지는 새로운 p진 수열군의 생성을 제안하였다.

본 논문의 마지막 결과는, 3진 m-수열과 이를 $d = \frac{3^{4k+2}-3^{2k+1}+3-1}{3+1} + 3^{2k+1}$으로 데시메이션한 수열간의 상호상관도에 대한 연구이다. 고려된 m-수열의 주기는 $3^{4+2} - 1$이며, 상호상관도의 상한 값은 $4.5 \cdot 3^{2k+1} + 1$으로 증명되었다. 증명 과정에는 이차형식에 대한 이론이 사용되었으며,

또한 Bluher [33]의 결과가 중요하게 이용되었다. 본 연구에서는 총 네 가지의 이차형식이 다루어졌으며 이는 일반적으로 이차형식을 이용한 상호상관도 연구에서 두 가지의 이차형식만 고려되는 것과 차별화된다.

주요어: 자기상관도, 상호상관도, 데시메이션 수열, 지수함수합, 클루스터만합, m-수열, 비이진수열, 의사난수수열, 이차형식, 수열군

학번: 2009-20782