RESULTS ON LCZ SEQUENCES AND QUADRATIC FORMS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

ELİF SAYGI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

NOVEMBER 2009

Approval of the thesis:

RESULTS ON LCZ SEQUENCES AND QUADRATIC FORMS

submitted by **ELİF SAYGI** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Ersan Akyıldız _____
Director, Graduate School of **Applied Mathematics**

Prof. Dr. Ferruh Özbudak _____
Head of Department, **Cryptography**

Prof. Dr. Ferruh Özbudak _____
Supervisor, **Department of Mathematics, METU**

Examining Committee Members:

Prof. Dr. Ersan Akyıldız _____
Department of Mathematics, METU

Prof. Dr. Ferruh Özbudak _____
Department of Mathematics, METU

Assoc. Prof. Dr. Ali Doğanaksoy _____
Department of Mathematics, METU

Assoc. Prof. Dr. Emrah Çakçak _____
Institute of Applied Mathematics, METU

Assist. Prof. Dr. Çetin Ürtiş _____
Department of Mathematics, TOBB ETU

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: ELİF SAYGI

Signature :

ABSTRACT

RESULTS ON LCZ SEQUENCES AND QUADRATIC FORMS

Saygı, Elif
Ph.D., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

November 2009, 71 pages

In this thesis we study low correlation zone (LCZ) sequence sets and a class of quadratic forms. In the first part we obtain two new classes of optimal LCZ sequence sets. In our first construction using a suitable orthogonal transformation we extend some results of [21]. We give new classes of LCZ sequence sets defined over $\mathbb{Z}_4$ in our second construction. We show that our LCZ sequence sets are optimal with respect to the Tang, Fan and Matsufiji bound [37]. In the second part we consider some special linearized polynomials and corresponding quadratic forms. We compute the number of solutions of certain equations related to these quadratic forms and we apply these result to obtain curves with many rational points.

Keywords: Sequences, LCZ sequences, Quadratic forms, Linearized polynomials

ÖZ

LCZ DİZİLERİ VE QUADRATİK FORMLAR ÜZERİNE SONUÇLAR

Saygı, Elif
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Kasım 2009, 71 sayfa

Bu tezde düşük korelasyon bölgesi (LCZ) dizi kümeleri ve quadratik formların bir sınıfını çalıştık. Birinci bölümde iki yeni en iyi LCZ dizi kümeleri sınıfları elde ettik. Birinci üretim metodumuzda uygun dik dönüşüm kullanarak, [21] de verilen bazı sonuçları genişlettik. İkinci üretim metodumuzda $\mathbb{Z}_4$ üzerinde tanımlı yeni LCZ dizi kümeleri sınıfları verdik. LCZ dizi kümelerimizin Tang, Fan and Matsufiji sınırına [37] göre en iyi olduklarını gösterdik. İkinci bölümde bazı özel doğrusallaştırılmış polinomlar ve karşı gelen quadratik formları göz önüne aldık. Bu quadratik formlarla ilişkili olan bazı denklemlerin çözüm sayılarını hesapladık ve bu sonuçları çok rasyonel noktası olan eğrileri elde etmek için kullandık.

Anahtar Kelimeler: Diziler, LCZ dizileri, Quadratik formlar, Doğrusallaştırılmış polinomlar

To My Lovely Son and Daughter: Emir Ali and Defne

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisor Prof. Dr. Ferruh Özbudak. His ideas and tremendous support had a major influence on this thesis.

A very special thanks goes to Prof. Dr. Ali Doğanaksoy. Everyday he encourage us and gives great motivation for our studies.

I would like to thank Prof. Dr. Ersan Akyıldız, who supports me during my studies.

Especially, I would like to give my special thanks to my husband Zülfükar whose patient love enabled me to complete this work.

I would also like to thank my family (İhsan, Aynur, Belgin, İsmail, Emir Ali, Defne) for the support they provided me through my entire life.

I deeply thank the members of the Institute of Applied Mathematics (especially Nejla Erdoğdu) and my friends for their supports during the period of my studies.

PREFACE

In this thesis we study low correlation zone (LCZ) sequence sets and a class of quadratic forms. In the first part we present two construction of LCZ sequence sets. The first construction extends the results of [21]. In this construction we use an orthogonal transformation and we note that this technique is used in [38] to obtain new quaternary sequences with optimal maximal correlation values. The second construction gives new classes of quaternary LCZ sequence sets. We explicitly compute the full auto-correlations and cross-correlations of the sequences in these sets. We show that our LCZ sequence sets in two constructions are optimal with respect to the Tang, Fan and Matsufiji bound [37] under some conditions.

In the second part we consider some special linearized polynomials and corresponding quadratic forms. We compute the number of solutions of certain equations related to these quadratic forms and we apply these result to obtain curves with many rational points. These results extend the results of [6].

This thesis is organized as follows: Chapter 1 gives a general background on sequences and quadratic forms. Our constructions of optimal LCZ sequence sets mentioned above are presented in Chapter 2. Chapter 3 deals with highly degenerate quadratic forms and gives the number of solutions of certain equations.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

CHAPTER 1

INTRODUCTION

This chapter presents a general background on sequences and quadratic forms. Our main concerns in this thesis are a special class of sequences called low correlation zone (LCZ) sequences and the number of solutions of certain equations. In Section 1.1 some basic definitions on sequences are given. Chapter 2 presents two distinct classes of optimal LCZ sequences. In Section 1.2 some basic definitions and notations on quadratic forms are given. Chapter 3 deals with a special type of quadratic forms. In this chapter we compute the number of solutions of certain equations related to these quadratic forms. Also we apply these result to obtain curves with many rational points.

1.1 An Introduction to Sequences

Let $F = \{\alpha_1, \alpha_2, \ldots\}$ be a set of distinct objects. A *sequence* is an ordered list of objects from the set F. The number of elements in a sequence is called the *length* of the sequence. Note that in many applications the cardinality of the set F is finite and in general F is chosen to a finite field or a Galois ring.

In cryptographic and coding theoretic applications, one wants to obtain sequences which have some specific properties, such as, large period, large linear complexity or linear span, low correlation etc. [11, 27].

Let $s = s_0, s_1, \ldots$ be a sequence of elements of F. If there exists integers $N > 0$ and $n_0 \geq 0$ such that $s_{i+N} = s_i$ for all $i \geq n_0$, and N is the smallest number having this property, then the sequence is called *ultimately periodic* with *period* N. Furthermore, if $n_0 = 0$ then an ultimately periodic sequence with period N is called *periodic* sequence with period N. A

significant property of periodic sequences is the correlation values of sequences. Formal definition of correlation of two sequences is given in Section 2.1.

In code-division multiple access (CDMA) communication systems sequences play an important role. They are assigned to distinct users in a common channel at the same time [33]. In order to distinguish each user and to minimize the interference we must use the sequences with the lowest possible non-trivial correlations. Furthermore, the capacity of the system can be increased by the number of sequences which support a larger number of distinct users. Since all users share the same bandwith, sequences can be eavesdropping. But if, sequences have large linear span then generating mechanisms can not be easily inferred by observing the sequences where linear span of a periodic sequence is the length of the shortest linear feedback shift register that can generate the sequence [18]. Consequently, a set of sequences with low correlation, large family size and large linear span plays an important role in CDMA communication systems.

Well known bounds for low correlation are derived by Welch, Sidelnikov and Levenshtein in [46, 32, 25]. Among the known optimal binary sequence families the most famous one is Gold Family, having $2^n + 1$ sequences with period $2^n - 1$ and having tree valued cross-correlation values achieving Sidelnikov bound for odd n in [10]. Kasami proposed in [17] sequences with optimal correlation achieving Welch's bound for even n. The other well known approaches are given in [2, 16, 22, 39, 44].

In 1990's optimal quaternary sequences were derived from Z_4 [1]. Family A is proposed in [1, 34] has family size $2^n + 1$, period $2^n - 1$ and maximum non-trivial correlation values are bounded by $2^{n/2} + 1$. Family B in [1] and Family C in [45] has family size 2^{n-1} and has period $2(2^n - 1)$. Tang and Udaya generalized the Family B and Family C to a new optimal quaternary Family D in [42]. Family D has the same period and the same maximal correlation values, but has 2^n sequences.

In 2009 Tang, Helleseth and Fan [38] proposed a general orthogonal transformation on the Family B and C which generates Family D and also yields a new optimal sequence Family E. Family E has the same period, same family size and same maximum correlation values with Family D. However, Family E has different correlation values from Family D. In Section 2.2 we use the same orthogonal transformation to extend the results given in [21].

In 1992, Gaudenzi, Elia and Viola [8] proposed the quasi-synchronous code-division multiple access (QS-CDMA) systems. In QS-CDMA systems relative time delay between the signature sequences of different users is random. But this time delay is restricted to certain time range L where L is much smaller than the period of the sequences used in system. Here we note that, in a general CDMA system L is equal to the period of the signature sequences.

As we stated above in CDMA systems it is important to use sequences having low correlation values. However, sequences used in QS-CDMA system must have low correlation values for some specific delays around the origin which are called low correlation zone (LCZ) sequences.

Let S be a set of M sequences with period N. If the magnitude of the non-trivial correlation value of two sequences in S takes values less than or equal to ϵ for the offset τ in the range $|\tau| < L$, then S is called a (N, M, L, ϵ) LCZ sequence set. A more formal definition is given in Definition 2.1.2.

In Chapter 2 we propose two constructions of LCZ sequence sets. In Section 2.2 we extend the results of [21] by using a suitable orthogonal transformation and note that this technique is used in [38] to obtain new quaternary sequences with optimal maximal correlation values. Furthermore, in Section 2.3 we present new classes of quaternary LCZ sequence sets. We explicitly compute the full auto-correlations and cross-correlations of the sequences in these sets. We show that our LCZ sequence sets are optimal with respect to the Tang, Fan and Matsufiji (2.1) bound under some conditions.

1.2 An Introduction to Quadratic Forms

In this section we introduce a class of quadratic forms that we study. Moreover we recall some basic definitions and we fix some notation. For details we refer to [26].

A quadratic form Q (in k indeterminates) over $\mathbb{F}_q$ is a homogeneous polynomial in the ring $\mathbb{F}_q[x_1, \ldots, x_k]$ of degree 2. Note that any element $x \in \mathbb{F}_{q^k}$ can be written as

$$x = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_k\alpha_k,$$

where the set $\{\alpha_1, \ldots, \alpha_k\}$ is a basis for $\mathbb{F}_{q^k}$. Therefore, Q can be written as

$$\begin{array}{rccc} Q: & \mathbb{F}_{q^k} & \to & \mathbb{F}_q \\ & x = \sum_{i=1}^{k} x_i \alpha_i & \mapsto & \sum_{i=1}^{k} \sum_{j=1}^{k} b_{i,j} x_i x_j, \end{array}$$

where $b_{i,j} \in \mathbb{F}_q$.

In the rest of this section we present some notations and some results considered in Chapter 3. Let

$$R(x) = s_0 x + s_1 x^q + \cdots + s_h x^{q^h} \in \mathbb{F}_{q^k}[x]$$

be an $\mathbb{F}_q$-linearized polynomial with $h \geq 0$ and $s_h \neq 0$.

Let $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ denotes the trace map from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$ given by

$$\begin{array}{rccc} \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q} : \mathbb{F}_{q^k} & \to & \mathbb{F}_q \\ x & \mapsto & x + x^q + \cdots + x^{q^{k-1}}. \end{array}$$

When it is clear from the context, we denote $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ as only Tr in short.

Let B_R be the symmetric bilinear form on the $\mathbb{F}_q$-linear vector space $\mathbb{F}_{q^k}$ defined as

$$\begin{array}{rccc} B_R : \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} & \to & \mathbb{F}_q \\ (x, y) & \mapsto & \mathrm{Tr}\left(xR(y) + yR(x)\right). \end{array}$$

Let Q_R be the quadratic form defined as

$$\begin{array}{rccc} Q_R : \mathbb{F}_{q^k} & \to & \mathbb{F}_q \\ x & \mapsto & \mathrm{Tr}\left(xR(x)\right). \end{array}$$

Let W_R be the radical of B_R, which is defined as

$$W_R = \{x \in \mathbb{F}_{q^k} : B_R(x, y) = 0 \quad \text{for each } y \in \mathbb{F}_{q^k}\}. \tag{1.1}$$

For $x \in \mathbb{F}_{q^k}$, we observe that $x \in W_S$ if and only if

$$\mathrm{Tr}(xR(y) + yR(x)) = \mathrm{Tr}\left(x\left(s_0 y + s_1 y^q + \cdots + s_h y^{q^h}\right) + y\left(s_0 x + s_1 x^q + \cdots + s_h x^{q^h}\right)\right) = 0$$

for all $y \in \mathbb{F}_{q^k}$. Note that

$$\mathrm{Tr}\left(xs_i y^{q^i}\right) = \mathrm{Tr}\left((xs_i)^{q^{-i}} y\right)$$

for all $i = 1, 2, \ldots, h$. Therefore, using this observation we can obtain that for $x \in \mathbb{F}_{q^k}$, $x \in W_R$ if and only if x is a root of the $\mathbb{F}_q$-linearized polynomial

$$\sum_{i=0}^{h-1} s_{h-i}^{q^i} T^{q^i} + 2s_0^{q^h} T^{q^h} + \sum_{i=1}^{h} s_i^{q^h} T^{q^{h+i}} \in \mathbb{F}_{q^k}[T]. \tag{1.2}$$

Let w be the $\mathbb{F}_q$-dimension

$$w := \dim_{\mathbb{F}_q} W_R$$

of W_R.

We can choose an $\mathbb{F}_q$-linear subspace $\overline{W}_R$ of $\mathbb{F}_{q^k}$ such that

$$W_R \oplus \overline{W}_R = \mathbb{F}_{q^k}.$$

In particular $\dim_{\mathbb{F}_q} \overline{W}_R = k - w$ and it is called the codimension of W_R.

It is known (cf. [26]) that any quadratic form has one of the following equivalent representation.

$$Q_R(x) = \begin{cases} x_{n+1}^2 + \sum_{i=1}^{n} x_i y_i \\ \sum_{i=1}^{n} x_i y_i \\ x_1^2 + s y_1^2 + \sum_{i=1}^{n} x_i y_i, \end{cases}$$

where $s \in \mathbb{F}_q$ is an element with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = s + s^2 + \cdots + s^{q/2} = 1$, w is the dimension of the radical W_R and $n = \dfrac{k-w}{2}$.

CHAPTER 2

LCZ SEQUENCE SETS

In this chapter we present two constructions of LCZ sequence sets. In Section 2.2 we extend the results of [21] by using an orthogonal transformation and note that this technique is used in [38] to obtain new quaternary sequences with optimal maximal correlation values. Given a LCZ sequence set V with parameters (N, M, L, ϵ) we construct a LCZ sequence set S with parameters $(2N, 2M, L, \epsilon)$ or $(2N, 2M, L-1, \epsilon)$ depending on L is odd or L is even respectively. Note that this construction method includes the construction in [21]. Furthermore, in Section 2.3 we give new classes of quaternary LCZ sequence sets. We explicitly compute the full auto-correlations and cross-correlations of the sequences in these sets. We show that our LCZ sequence sets are optimal with respect to the Tang, Fan and Matsufiji bound (2.1) under some conditions.

Quasi-synchous code-division multiple access (QS-CDMA) communication systems are proposed by Gaudenzi, Elia and Viola [8]. In a QS-CDMA system, performance is determined by the correlation value around the origin, rather than the overall correlation value. Therefore, LCZ sequences are good candidates for such systems.

Recently there have been many developments on the design of LCZ sequence sets. Tang and Fan [36] proposed a LCZ sequence set over GF(p), based on Gordon-Mills-Welch (GMW) [13] sequences. Kim, Jang, No and Chung [20] proposed a new quaternary LCZ sequence set from binary sequences with ideal auto-correlation. These sequences are optimal with respect to Tang, Fan and Matsufuji bound (2.1). Jang, No and Chung [14] proposed an optimal p^2-ary LCZ sequence set, which can be viewed as the generalization of the work in [20]. Tang and Udaya [40] proposed a new binary LCZ sequence set derived from interleaved technique and Hadamard matrices. Later they design a recursive construction method for optimal LCZ

sequence set in [41]. Kim, Jang, No and Chung [21] proposed a new design scheme for binary LCZ sequence sets and proposed an extension method with even alphabet size. Jang, No, Chung and Tang [15] constructed optimal p-ary LCZ sequences. Gong, Golomb and Song [12] presented a general approach to the design of LCZ sequences. Constructions in [14, 15, 20, 36, 41] can be obtained by this general setting. Zhou, Tang and Gong [47] proposed a new method of construction LCZ sequence set. For binary LCZ sequence sets this result is better than those in [21]. Recently Chung and Yang [4] proposed a construction method for quaternary LCZ sequence sets from binary sequences with good auto-correlation.

This chapter is organized as follows: In Section 2.1 we introduce some basic definitions and some notations. In Section 2.2, we present our first construction which extends the construction given in [21]. Furthermore, we present our second construction in Section 2.3.

2.1 Preliminaries

In this section we introduce some basic definitions and we fix some notations.

Let $q = 2^t$ for some positive integer t. For positive integer n let $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$ denote the finite fields with q and q^n elements. Recall that $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ denotes the trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ given by

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n} &\rightarrow \mathbb{F}_q \\ x &\mapsto x + x^q + \cdots + x^{q^{n-1}}. \end{aligned}$$

Throughout the chapter for a finite field $\mathbb{F}_q$, we denote its multiplicative group $\mathbb{F}_q \setminus \{0\}$ as $\mathbb{F}_q^*$, and when it is clear from context, we also denote $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ as only Tr in short.

Here we note that the sequences defined over $\mathbb{Z}_q$ are called *q-ary sequences*. A special class of q-ary sequences are the ones defined over $\mathbb{Z}_4$ and such sequences are called *quaternary sequences*. A (periodic) correlation of q-ary sequences is defined as follows:

Definition 2.1.1 *Let $s_i(t)$ and $s_j(t)$ be two q-ary sequences of period N. The correlation between $s_i(t)$ and $s_j(t)$ at shift τ, is defined as*

$$R_{i,j}(\tau) = \sum_{t=0}^{N-1} \omega^{s_i(t) - s_j(t+\tau)}$$

where $\omega = e^{\frac{2\pi\sqrt{-1}}{q}}$ *is a complex qth root of unity and* $t + \tau$ *is computed modulo* N.

Note that if $s_i(t)$ and $s_j(t)$ are *cyclically equivalent*, i.e., $s_i(t) = s_j(t + t')$ for all $1 \leq t, t' \leq N$, then $R_{i,j}$ is called the auto-correlation of $s_i(t)$. Otherwise, if $s_i(t)$ and $s_j(t)$ are cyclically distinct, then $R_{i,j}$ is called the cross-correlation of $s_i(t)$ and $s_j(t)$.

Here we remark that the correlation can also be defined if the sequences are defined over $\mathbb{F}_q$ [12]. As it is noted in [12] using a one to one correspondence between $\mathbb{Z}_q$ and $\mathbb{F}_q$ if one derives the cross-correlation between the sequences defined over $\mathbb{Z}_q$, then at the same time one obtains the cross-correlation between the sequences defined over $\mathbb{F}_q$.

Now we present a formal definition of a LCZ sequence set.

Definition 2.1.2 *Let* S *be a set of* M *q-ary sequences of period* N. *Then* S *is called a low correlation zone (or LCZ in short) sequence set having parameters* (N, M, L, ϵ)*, if for any two sequences* $s_i(t), s_j(t) \in S$ *we have*

$$|R_{i,j}(\tau)| \leq \epsilon \quad \textit{for } (i \neq j \textit{ and } |\tau| < L) \textit{ or } (i = j \textit{ and } 0 \neq |\tau| < L)\,.$$

The following lower bound for the parameters of a LCZ sequence set is given in [37]. We will use this result to show the optimality of our LCZ sequence sets.

Theorem 2.1.3 *[37] Let* S *be an LCZ sequence set with parameters* (N, M, L, ϵ). *Then we have*

$$ML - 1 \leq \frac{N(N-1)}{N - \epsilon^2}. \tag{2.1}$$

Now we describe a general orthogonal transformation given in [38]. Assume that we have a q-ary sequence set V given as

$$V = \{v_i(t) | 0 \leq i \leq M-1, \quad 0 \leq t \leq N-1\}.$$

In order to obtain a sequence set S having $2M$ sequences of period $2N$, the following general transformation on V can be used. Let $(c_{0,0}, c_{0,1}, c_{1,0}, c_{1,1}) \in \mathbb{Z}_q^4$, define

$$S = \{s_{i,j}(t) | 0 \leq i \leq M-1, \quad 0 \leq j \leq 1 \quad 0 \leq t \leq 2N-1\} \tag{2.2}$$

where $s_{i,j}(t)$ is

$$s_{i,j}(t) = \begin{cases} v_i(t_1) + c_{j,0} & \text{if } t = 2t_1, \\ v_i\left(t_1 + \left\lceil \frac{L}{2} \right\rceil\right) + c_{j,1} & \text{if } t = 2t_1 + 1. \end{cases} \tag{2.3}$$

Note that $\lceil x \rceil$ denotes the smallest integer greater than or equal to x and the construction in [21] is a special case of (2.3) with $(c_{0,0}, c_{0,1}, c_{1,0}, c_{1,1}) = \left(0, 0, \frac{q}{2}, 0\right)$. Furthermore, any two sequences are called equivalent if the one is obtained by adding a constant to each term of the other sequence. In our case, if $s_{i,j}$ and $s'_{i,j}$ are two equivalent sequences in S we have $s_{i,j} = s'_{i,j} + c$, that is, $c_{j,0} = c_{j,1} = c$. Therefore, the pair $(c_{j,0}, c_{j,1})$ can always be normalized by setting $c_{j,1} = 0$, that is,

$$\begin{pmatrix} c_{0,0} & c_{0,1} \\ c_{1,0} & c_{1,1} \end{pmatrix} = \begin{pmatrix} c_0 & 0 \\ c_1 & 0 \end{pmatrix}.$$

In the following section, we obtain LCZ sequence sets by using this orthogonal transformation under the condition that $c_0 - c_1 \equiv \frac{q}{2} \mod q$. This condition is a necessary and sufficient condition to obtain LCZ sequence sets.

2.2 Extensions of LCZ Sequence Sets

Let q be an even integer. Assume that we have a LCZ sequence set V with parameters (N, M, L, ϵ) given as

$$V = \{v_i(t) | 0 \le i \le M - 1, \quad 0 \le t \le N - 1\}. \tag{2.4}$$

Now in the following construction we use the orthogonal transformation described in the previous section to extend the above LCZ sequence set V in (2.4). The parameters of the new LCZ sequence set becomes $(2N, 2M, L, 2\epsilon)$ or $(2N, 2M, L - 1, 2\epsilon)$ depending L is odd or L is even respectively.

Construction 2.2.1 *Let S be the set of q-ary sequences defined as*

$$S = \{s_i(t) | 0 \le i \le 2M - 1, \quad 0 \le t \le 2N - 1\} \tag{2.5}$$

where $s_i(t)$ *is*

$$\begin{aligned} s_i(2t_1) &= \begin{cases} v_i(t_1) + c_0 & \text{for } 0 \le i \le M-1, \\ v_{i-M}(t_1) + c_1 & \text{for } M \le i \le 2M-1, \end{cases} \\ s_i(2t_1+1) &= \begin{cases} v_i\left(t_1 + \left\lceil \frac{L}{2} \right\rceil\right) & \text{for } 0 \le i \le M-1, \\ v_{i-M}\left(t_1 + \left\lceil \frac{L}{2} \right\rceil\right) & \text{for } M \le i \le 2M-1. \end{cases} \end{aligned} \tag{2.6}$$

provided that $c_0 - c_1 \equiv \frac{q}{2} \mod q$.

Now we are ready to give our main result of this section.

Theorem 2.2.2 *The set S in Construction 2.2.1 is a LCZ sequence set with parameters* $(2N, 2M, L, 2\epsilon)$ *if L is odd and with parameters* $(2N, 2M, L-1, 2\epsilon)$ *if L is even.*

In the following two subsections we will give the proof of Theorem 2.2.2, considering the cases L is odd and L is even separately.

2.2.1 Case: L is odd

In this section we will prove Theorem 2.2.2 for the case L is odd. Assume that $L = 2L_1 - 1$ for some integer L_1. Then we have that

$$\left\lceil \frac{L}{2} \right\rceil = \frac{L+1}{2} = L_1.$$

Recall that $R_{i,j}(\tau)$ is the correlation between two sequences $s_i(t)$ and $s_j(t)$ at shift τ given as

$$R_{i,j}(\tau) = \sum_{t=0}^{2N-1} \omega^{s_i(t) - s_j(t+\tau)}$$

where ω is a complex qth root of unity. Now considering the definition of sequences in Construction 2.2.1 we can rewrite the correlation between two sequences $s_i(t)$ and $s_j(t)$ as

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{2N-1} \omega^{s_i(t) - s_j(t+\tau)} \\ &= \sum_{t=0}^{N-1} \omega^{s_i(2t) - s_j(2t+\tau)} + \sum_{t=0}^{N-1} \omega^{s_i(2t+1) - s_j(2t+1+\tau)} \end{aligned} \tag{2.7}$$

which is more useful for our computations.

Now for the simplicity of the proof we must consider the following eight cases separately.

Case 1. $0 \leq i, j < M$ and τ is even.

Assume that $\tau = 2\tau_1$. In this case, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_i(t)+c_0-v_j(t+\tau_1)-c_0} + \sum_{t=0}^{N-1} \omega^{v_i(t+L_1)-v_j(t+L_1+\tau_1)} \\ &= \sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1)} + \sum_{t=L_1}^{N-1+L_1} \omega^{v_i(t)-v_j(t+\tau_1)} \\ &= \sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1)} + \sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1)}, \end{aligned}$$

as $v_i(t)$ has period N. Now using the property that V is an (N, M, L, ϵ) LCZ sequence set and Definition 2.1.2,

$$\left|\sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1)}\right| \leq \epsilon \quad \text{for } (i \neq j \text{ and } |\tau_1| < L) \text{ or } (i = j \text{ and } 0 \neq |\tau_1| < L).$$

Therefore,

$$\begin{aligned} \left|R_{i,j}(\tau)\right| &= \left|\sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1)} + \sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1)}\right| \\ &\leq \left|\sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1)}\right| + \left|\sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1)}\right| \\ &\leq \epsilon + \epsilon = 2\epsilon, \end{aligned}$$

for $(i \neq j$ and $|\tau_1| < L)$ or $(i = j$ and $0 \neq |\tau_1| < L)$.

Hence,

$$\left|R_{i,j}(\tau)\right| \leq 2\epsilon \quad \text{for } (i \neq j \text{ and } |\tau| < 2L) \text{ or } (i = j \text{ and } 0 \neq |\tau| < 2L).$$

Case 2. $0 \leq i, j < M$ and τ is odd.

Assume that $\tau = 2\tau_1 + 1$. In this case, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_i(t)+c_0-v_j(t+\tau_1+L_1)} + \sum_{t=0}^{N-1} \omega^{v_i(t+L_1)-v_j(t+\tau_1+1)-c_0} \\ &= \omega^{c_0} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1+L_1)} + \omega^{-c_0} \sum_{t=L_1}^{N-1+L_1} \omega^{v_i(t)-v_j(t-L_1+\tau_1+1)} \\ &= \omega^{c_0} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1+L_1)} + \omega^{-c_0} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t-L_1+\tau_1+1)}, \end{aligned} \tag{2.8}$$

as $v_i(t)$ has period N. Now using the property that V is an (N, M, L, ϵ) LCZ sequence set and Definition 2.1.2, for the first summation in (2.8) we have

$$\left|\sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1+L_1)}\right| \leq \epsilon \quad \text{for } (i \neq j \text{ and } |\tau_1 + L_1| < L) \text{ or } (i = j \text{ and } 0 \neq |\tau_1 + L_1| < L).$$

Now replacing $L = 2L_1 - 1$ and $\tau = 2\tau_1 + 1$, the condition

$$|\tau_1 + L_1| < L$$

becomes

$$\left|\frac{\tau - 1}{2} + \frac{L + 1}{2}\right| < L,$$

which implies that

$$-3L < \tau < L.$$

Similarly, the condition

$$0 \neq |\tau_1 + L_1| < L$$

becomes

$$\tau_1 \neq -L_1 \quad \text{and } -3L < \tau < L,$$

which implies that

$$\tau \neq -L \quad \text{and } -3L < \tau < L.$$

Therefore the first summation in (2.8) becomes

$$\left|\sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1+L_1)}\right| \leq \epsilon \quad \text{for } (|\tau| < L). \tag{2.9}$$

For the second summation in (2.8) we have

$$\left|\sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t-L_1+\tau_1+1)}\right| \leq \epsilon \quad \text{for} \quad (i \neq j \text{ and } |-L_1 + \tau_1 + 1| < L) \text{ or}$$
$$(i = j \text{ and } 0 \neq |-L_1 + \tau_1 + 1| < L).$$

Now replacing $L = 2L_1 - 1$ and $\tau = 2\tau_1 + 1$, the condition

$$|-L_1 + \tau_1 + 1| < L$$

becomes

$$\left|-\frac{L+1}{2}+\frac{\tau-1}{2}+1\right|<L,$$

which implies that

$$-L<\tau<3L.$$

Similarly, the condition

$$0\neq|-L_1+\tau_1+1|<L$$

becomes

$$\tau_1\neq L_1-1 \quad \text{and } -L<\tau<3L,$$

which implies that

$$\tau\neq L \quad \text{and } -L<\tau<3L.$$

Therefore the second summation in (2.8) becomes

$$\left|\sum_{t=0}^{N-1}\omega^{v_i(t)-v_j(t-L_1+\tau_1+1)}\right|\leq\epsilon \quad \text{for } (|\tau|<L). \tag{2.10}$$

Now combining (2.8), (2.9) and (2.10) we have

$$\begin{aligned}\left|R_{i,j}(\tau)\right| &= \left|\omega^{c_0}\sum_{t=0}^{N-1}\omega^{v_i(t)-v_j(t+\tau_1+L_1)}+\omega^{-c_0}\sum_{t=0}^{N-1}\omega^{v_i(t)-v_j(t-L_1+\tau_1+1)}\right| \\ &\leq \left|\omega^{c_0}\right|\left|\sum_{t=0}^{N-1}\omega^{v_i(t)-v_j(t+\tau_1+L_1)}\right|+\left|\omega^{-c_0}\right|\left|\sum_{t=0}^{N-1}\omega^{v_i(t)-v_j(t-L_1+\tau_1+1)}\right| \\ &\leq 1\cdot\epsilon+1\cdot\epsilon=2\epsilon \quad \text{for } (|\tau|<L).\end{aligned}$$

Case 3. $0\leq i<M, M\leq j<2M$ and τ is even.

Assume that $\tau=2\tau_1$. In this case, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned}R_{i,j}(\tau) &= \sum_{t=0}^{N-1}\omega^{v_i(t)+c_0-v_{j-M}(t+\tau_1)-c_1}+\sum_{t=0}^{N-1}\omega^{v_i(t+L_1)-v_{j-M}(t+L_1+\tau_1)} \\ &= \omega^{c_0-c_1}\sum_{t=0}^{N-1}\omega^{v_i(t)-v_{j-M}(t+\tau_1)}+\sum_{t=0}^{N-1}\omega^{v_i(t)-v_{j-M}(t+\tau_1)} \\ &= -\sum_{t=0}^{N-1}\omega^{v_i(t)-v_{j-M}(t+\tau_1)}+\sum_{t=0}^{N-1}\omega^{v_i(t)-v_{j-M}(t+\tau_1)}=0,\end{aligned}$$

as $v_i(t)$ has period N and $\omega^{c_0-c_1} = -1$ by the assumption $c_0 - c_1 \equiv \frac{q}{2} \mod q$ in the Construction 2.2.1.

Hence,

$$\left|R_{i,j}(\tau)\right| = 0 \leq 2\epsilon \quad \text{for } (|\tau| < 2L).$$

Case 4. $0 \leq i < M, M \leq j < 2M$ and τ is odd.

Assume that $\tau = 2\tau_1 + 1$. In this case, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_i(t)+c_0-v_{j-M}(t+\tau_1+L_1)} + \sum_{t=0}^{N-1} \omega^{v_i(t+L_1)-v_{j-M}(t+\tau_1+1)-c_1} \\ &= \omega^{c_0} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t+\tau_1+L_1)} + \omega^{-c_1} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t-L_1+\tau_1+1)} \end{aligned} \tag{2.11}$$

as $v_i(t)$ has period N.

Now we observe that (2.9) and (2.10) are again valid for $|\tau| < L$. Therefore, using (2.9), (2.10) and (2.11) we obtain that

$$\begin{aligned} \left|R_{i,j}(\tau)\right| &= \left|\omega^{c_0} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t+\tau_1+L_1)} + \omega^{-c_1} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t-L_1+\tau_1+1)}\right| \\ &\leq \left|\omega^{c_0}\right| \left|\sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t+\tau_1+L_1)}\right| + \left|\omega^{-c_1}\right| \left|\sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t-L_1+\tau_1+1)}\right| \\ &\leq 1 \cdot \epsilon + 1 \cdot \epsilon = 2\epsilon \quad \text{for } (|\tau| < L). \end{aligned}$$

Case 5. $M \leq i < 2M, 0 \leq j < M$ and τ is even.

Assume that $\tau = 2\tau_1$. In this case, similar to the proof of Case 3, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)+c_1-v_j(t+\tau_1)-c_0} + \sum_{t=0}^{N-1} \omega^{v_{i-M}(t+L_1)-v_j(t+L_1+\tau_1)} \\ &= \omega^{c_1-c_0} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t+\tau_1)} + \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t+\tau_1)} = 0, \end{aligned}$$

as $v_i(t)$ has period N and $\omega^{c_0-c_1} = -1$. Hence, we obtain that

$$\left|R_{i,j}(\tau)\right| = 0 \leq 2\epsilon \quad \text{for } (|\tau| < 2L).$$

Case 6. $M \le i < 2M, 0 \le j < M$ and τ is odd.

Assume that $\tau = 2\tau_1 + 1$. In this case, similar to the proof of Case 4, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)+c_1-v_j(t+\tau_1+L_1)} + \sum_{t=0}^{N-1} \omega^{v_{i-M}(t+L_1)-v_j(t+\tau_1+1)-c_0} \\ &= \omega^{c_1} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t+\tau_1+L_1)} + \omega^{-c_0} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t-L_1+\tau_1+1)} \end{aligned}$$

as $v_i(t)$ has period N. By the same reasoning as in Case 4, we have

$$\begin{aligned} \left|R_{i,j}(\tau)\right| &= \left| \omega^{c_1} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t+\tau_1+L_1)} + \omega^{-c_0} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t-L_1+\tau_1+1)} \right| \\ &\le \left|\omega^{c_1}\right| \left| \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t+\tau_1+L_1)} \right| + \left|\omega^{-c_0}\right| \left| \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t-L_1+\tau_1+1)} \right| \\ &\le 1 \cdot \epsilon + 1 \cdot \epsilon = 2\epsilon \quad \text{for } (|\tau| < L)\,. \end{aligned}$$

Case 7. $M \le i, j < 2M$ and τ is even.

Assume that $\tau = 2\tau_1$. In this case, similar to the proof of Case 1, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)+c_1-v_{j-M}(t+\tau_1)-c_1} + \sum_{t=0}^{N-1} \omega^{v_{i-M}(t+L_1)-v_{j-M}(t+L_1+\tau_1)} \\ &= \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_{j-M}(t+\tau_1)} + \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_{j-M}(t+\tau_1)}, \end{aligned}$$

as $v_i(t)$ has period N. By the same reasoning as in Case 1, we have

$$\left|R_{i,j}(\tau)\right| \le 2\epsilon \quad \text{for } (i \ne j \text{ and } |\tau| < 2L) \text{ or } (i = j \text{ and } 0 \ne |\tau| < 2L)\,.$$

Case 8. $M \le i, j < 2M$ and τ is odd.

Assume that $\tau = 2\tau_1 + 1$. In this case, similar to the proof of Case 2, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)+c_1-v_{j-M}(t+\tau_1+L_1)} + \sum_{t=0}^{N-1} \omega^{v_{i-M}(t+L_1)-v_{j-M}(t+\tau_1+1)-c_1} \\ &= \omega^{c_1} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_{j-M}(t+\tau_1+L_1)} + \omega^{-c_1} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_{j-M}(t-L_1+\tau_1+1)} \end{aligned}$$

as $v_i(t)$ has period N. By the same reasoning as in Case 2, and using (2.9) and (2.10) we have

$$\begin{aligned}
\left|R_{i,j}(\tau)\right| &= \left|\omega^{c_1}\sum_{t=0}^{N-1}\omega^{v_{i-M}(t)-v_{j-M}(t+\tau_1+L_1)} + \omega^{-c_1}\sum_{t=0}^{N-1}\omega^{v_{i-M}(t)-v_{j-M}(t-L_1+\tau_1+1)}\right| \\
&\leq \left|\omega^{c_1}\right|\left|\sum_{t=0}^{N-1}\omega^{v_{i-M}(t)-v_{j-M}(t+\tau_1+L_1)}\right| + \left|\omega^{-c_1}\right|\left|\sum_{t=0}^{N-1}\omega^{v_{i-M}(t)-v_{j-M}(t-L_1+\tau_1+1)}\right| \\
&\leq 1\cdot\epsilon + 1\cdot\epsilon = 2\epsilon \quad \text{for } (|\tau| < L)\,.
\end{aligned}$$

As a result of the above eight cases, we obtain that for any two sequences $s_i(t), s_j(t) \in S$ we have

$$|R_{i,j}(\tau)| \leq \epsilon \quad \text{for } (i \neq j \text{ and } |\tau| < L) \text{ or } (i = j \text{ and } 0 \neq |\tau| < L)\,.$$

Therefore, S is a LCZ sequence set having parameters $(2N, 2M, L, 2\epsilon)$, which completes the proof of Theorem 2.2.2 for the case L is odd.

2.2.2 Case: L is even

In this section we will prove Theorem 2.2.2 for the case L is even. The proof is similar to the previous case where L is odd. Now assume that $L = 2L_1$ for some integer L_1. Then we have that

$$\left\lceil \frac{L}{2} \right\rceil = \frac{L}{2} = L_1.$$

Again for the simplicity of the proof we must consider the following eight cases separately.

Case 1. $0 \leq i, j < M$ and τ is even.

Assume that $\tau = 2\tau_1$. In this case, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned}
R_{i,j}(\tau) &= \sum_{t=0}^{N-1}\omega^{v_i(t)+c_0-v_j(t+\tau_1)-c_0} + \sum_{t=0}^{N-1}\omega^{v_i(t+L_1)-v_j(t+L_1+\tau_1)} \\
&= \sum_{t=0}^{N-1}\omega^{v_i(t)-v_j(t+\tau_1)} + \sum_{t=0}^{N-1}\omega^{v_i(t)-v_j(t+\tau_1)},
\end{aligned}$$

as $v_i(t)$ has period N. By the same reasoning as in Case 1 of the Case L is odd, we have

$$\left|R_{i,j}(\tau)\right| \leq 2\epsilon \quad \text{for } (i \neq j \text{ and } |\tau| < 2L) \text{ or } (i = j \text{ and } 0 \neq |\tau| < 2L)\,.$$

Case 2. $0 \leq i, j < M$ and τ is odd.

Assume that $\tau = 2\tau_1 + 1$. In this case, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_i(t)+c_0-v_j(t+\tau_1+L_1)} + \sum_{t=0}^{N-1} \omega^{v_i(t+L_1)-v_j(t+\tau_1+1)-c_0} \\ &= \omega^{c_0} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1+L_1)} + \omega^{-c_0} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t-L_1+\tau_1+1)} \end{aligned} \tag{2.12}$$

as $v_i(t)$ has period N. Now using the property that V is an (N, M, L, ϵ) LCZ sequence set and Definition 2.1.2, for the first summation in (2.12) we have

$$\left| \sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1+L_1)} \right| \leq \epsilon \quad \text{for } (i \neq j \text{ and } |\tau_1 + L_1| < L) \text{ or } (i = j \text{ and } 0 \neq |\tau_1 + L_1| < L).$$

Now replacing $L = 2L_1$ and $\tau = 2\tau_1 + 1$, the condition

$$|\tau_1 + L_1| < L$$

becomes

$$\left| \frac{\tau - 1}{2} + \frac{L}{2} \right| < L,$$

which implies that

$$-3L + 1 < \tau < L + 1.$$

Similarly, the condition

$$0 \neq |\tau_1 + L_1| < L$$

becomes

$$\tau_1 \neq -L_1 \quad \text{and } -3L + 1 < \tau < L + 1,$$

which implies that

$$\tau \neq -L + 1 \quad \text{and } -3L + 1 < \tau < L + 1.$$

Therefore the first summation in (2.12) becomes

$$\left| \sum_{t=0}^{N-1} \omega^{v_i(t)-v_j(t+\tau_1+L_1)} \right| \leq \epsilon \quad \text{for } (|\tau| < L - 1). \tag{2.13}$$

For the second summation in (2.12) we have

$$\left|\sum_{t=0}^{N-1}\omega^{v_i(t)-v_j(t-L_1+\tau_1+1)}\right| \le \epsilon \quad \text{for} \qquad (i \ne j \text{ and } |-L_1+\tau_1+1| < L) \text{ or}$$
$$(i = j \text{ and } 0 \ne |-L_1+\tau_1+1| < L)\,.$$

Now replacing $L = 2L_1$ and $\tau = 2\tau_1 + 1$, the condition

$$|-L_1+\tau_1+1| < L$$

becomes

$$\left|-\frac{L}{2}+\frac{\tau-1}{2}+1\right| < L,$$

which implies that

$$-L-1 < \tau < 3L-1.$$

Similarly, the condition

$$0 \ne |-L_1+\tau_1+1| < L$$

becomes

$$\tau_1 \ne L_1 - 1 \quad \text{and } -L-1 < \tau < 3L-1,$$

which implies that

$$\tau \ne L-1 \quad \text{and } -L-1 < \tau < 3L-1.$$

Therefore the second summation in (2.12) becomes

$$\left|\sum_{t=0}^{N-1}\omega^{v_i(t)-v_j(t-L_1+\tau_1+1)}\right| \le \epsilon \quad \text{for } (|\tau| < L-1)\,. \tag{2.14}$$

Now combining (2.12), (2.13) and (2.14) we have

$$\begin{aligned}
\left|R_{i,j}(\tau)\right| &= \left|\omega^{c_0}\sum_{t=0}^{N-1}\omega^{v_i(t)-v_j(t+\tau_1+L_1)} + \omega^{-c_0}\sum_{t=0}^{N-1}\omega^{v_i(t)-v_j(t-L_1+\tau_1+1)}\right| \\
&\le \left|\omega^{c_0}\right|\left|\sum_{t=0}^{N-1}\omega^{v_i(t)-v_j(t+\tau_1+L_1)}\right| + \left|\omega^{-c_0}\right|\left|\sum_{t=0}^{N-1}\omega^{v_i(t)-v_j(t-L_1+\tau_1+1)}\right| \\
&\le 1\cdot\epsilon + 1\cdot\epsilon = 2\epsilon \quad \text{for } (|\tau| < L-1)\,.
\end{aligned}$$

Case 3. $0 \le i < M, M \le j < 2M$ and τ is even.

Assume that $\tau = 2\tau_1$. In this case, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_i(t)+c_0-v_{j-M}(t+\tau_1)-c_1} + \sum_{t=0}^{N-1} \omega^{v_i(t+L_1)-v_{j-M}(t+L_1+\tau_1)} \\ &= \omega^{c_0-c_1} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t+\tau_1)} + \sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t+\tau_1)} = 0, \end{aligned}$$

as $v_i(t)$ has period N and $\omega^{c_0-c_1} = -1$. Hence, we have

$$\left|R_{i,j}(\tau)\right| = 0 \le 2\epsilon \quad \text{for } (|\tau| < 2L).$$

Case 4. $0 \le i < M, M \le j < 2M$ and τ is odd.

Assume that $\tau = 2\tau_1 + 1$. In this case, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_i(t)+c_0-v_{j-M}(t+\tau_1+L_1)} + \sum_{t=0}^{N-1} \omega^{v_i(t+L_1)-v_{j-M}(t+\tau_1+1)-c_1} \\ &= \omega^{c_0} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t+\tau_1+L_1)} + \omega^{-c_1} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t-L_1+\tau_1+1)} \end{aligned} \tag{2.15}$$

as $v_i(t)$ has period N.

Now we observe that (2.13) and (2.14) are again valid for $|\tau| < L - 1$. Therefore, using (2.13), (2.14) and (2.15) we obtain that

$$\begin{aligned} \left|R_{i,j}(\tau)\right| &= \left| \omega^{c_0} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t+\tau_1+L_1)} + \omega^{-c_1} \sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t-L_1+\tau_1+1)} \right| \\ &\le \left|\omega^{c_0}\right| \left| \sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t+\tau_1+L_1)} \right| + \left|\omega^{-c_1}\right| \left| \sum_{t=0}^{N-1} \omega^{v_i(t)-v_{j-M}(t-L_1+\tau_1+1)} \right| \\ &\le 1 \cdot \epsilon + 1 \cdot \epsilon = 2\epsilon \quad \text{for } (|\tau| < L - 1). \end{aligned}$$

Case 5. $M \le i < 2M, 0 \le j < M$ and τ is even.

Assume that $\tau = 2\tau_1$. In this case, similar to the proof of Case 3, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)+c_1-v_j(t+\tau_1)-c_0} + \sum_{t=0}^{N-1} \omega^{v_{i-M}(t+L_1)-v_j(t+L_1+\tau_1)} \\ &= \omega^{c_1-c_0} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t+\tau_1)} + \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t+\tau_1)} = 0, \end{aligned}$$

as $v_i(t)$ has period N and $\omega^{c_0-c_1} = -1$. Hence, we obtain that

$$\left|R_{i,j}(\tau)\right| = 0 \le 2\epsilon \quad \text{for } (|\tau| < 2L)\,.$$

Case 6. $M \le i < 2M, 0 \le j < M$ and τ is odd.

Assume that $\tau = 2\tau_1 + 1$. In this case, similar to the proof of Case 4, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)+c_1-v_j(t+\tau_1+L_1)} + \sum_{t=0}^{N-1} \omega^{v_{i-M}(t+L_1)-v_j(t+\tau_1+1)-c_0} \\ &= \omega^{c_1} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t+\tau_1+L_1)} + \omega^{-c_0} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t-L_1+\tau_1+1)} \end{aligned}$$

as $v_i(t)$ has period N. By the same reasoning as in Case 4, we have

$$\begin{aligned} \left|R_{i,j}(\tau)\right| &= \left|\omega^{c_1} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t+\tau_1+L_1)} + \omega^{-c_0} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t-L_1+\tau_1+1)}\right| \\ &\le \left|\omega^{c_1}\right| \left|\sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t+\tau_1+L_1)}\right| + \left|\omega^{-c_0}\right| \left|\sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_j(t-L_1+\tau_1+1)}\right| \\ &\le 1 \cdot \epsilon + 1 \cdot \epsilon = 2\epsilon \quad \text{for } (|\tau| < L-1)\,. \end{aligned}$$

Case 7. $M \le i, j < 2M$ and τ is even.

Assume that $\tau = 2\tau_1$. In this case, similar to the proof of Case 1, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)+c_1-v_{j-M}(t+\tau_1)-c_1} + \sum_{t=0}^{N-1} \omega^{v_{i-M}(t+L_1)-v_{j-M}(t+L_1+\tau_1)} \\ &= \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_{j-M}(t+\tau_1)} + \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_{j-M}(t+\tau_1)}, \end{aligned}$$

as $v_i(t)$ has period N. By the same reasoning as in Case 1, we have

$$\left|R_{i,j}(\tau)\right| \le 2\epsilon \quad \text{for } (i \ne j \text{ and } |\tau| < 2L) \text{ or } (i = j \text{ and } 0 \ne |\tau| < 2L)\,.$$

Case 8. $M \le i, j < 2M$ and τ is odd.

Assume that $\tau = 2\tau_1 + 1$. In this case, similar to the proof of Case 2, $R_{i,j}(\tau)$ in (2.7) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)+c_1-v_{j-M}(t+\tau_1+L_1)} + \sum_{t=0}^{N-1} \omega^{v_{i-M}(t+L_1)-v_{j-M}(t+\tau_1+1)-c_1} \\ &= \omega^{c_1} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_{j-M}(t+\tau_1+L_1)} + \omega^{-c_1} \sum_{t=0}^{N-1} \omega^{v_{i-M}(t)-v_{j-M}(t-L_1+\tau_1+1)} \end{aligned}$$

as $v_i(t)$ has period N. By the same reasoning as in Case 2, and using (2.13) and (2.14) we have

$$\begin{aligned}
\left|R_{i,j}(\tau)\right| &= \left|\omega^{c_1}\sum_{t=0}^{N-1}\omega^{v_{i-M}(t)-v_{j-M}(t+\tau_1+L_1)} + \omega^{-c_1}\sum_{t=0}^{N-1}\omega^{v_{i-M}(t)-v_{j-M}(t-L_1+\tau_1+1)}\right| \\
&\leq \left|\omega^{c_1}\right|\left|\sum_{t=0}^{N-1}\omega^{v_{i-M}(t)-v_{j-M}(t+\tau_1+L_1)}\right| + \left|\omega^{-c_1}\right|\left|\sum_{t=0}^{N-1}\omega^{v_{i-M}(t)-v_{j-M}(t-L_1+\tau_1+1)}\right| \\
&\leq 1\cdot\epsilon + 1\cdot\epsilon = 2\epsilon \quad \text{for } (|\tau| < L-1)\,.
\end{aligned}$$

As a result of the above eight cases, we obtain that for any two sequences $s_i(t), s_j(t) \in S$ we have

$$|R_{i,j}(\tau)| \leq \epsilon \quad \text{for } (i \neq j \text{ and } |\tau| < L) \text{ or } (i = j \text{ and } 0 \neq |\tau| < L-1)\,.$$

Therefore, S is a LCZ sequence set having parameters $(2N, 2M, L-1, 2\epsilon)$, which completes the proof of Theorem 2.2.2 for the case L is even.

Therefore we complete the proof of Theorem 2.2.2 for all cases.

For the optimality of our LCZ sequence set the following corollary gives the condition on the parameters N, M and L.

Corollary 2.2.3 *[21, Corollary 13] Assume that the sequence set V in (2.4) is an optimal $(N, M, L, 1)$ LCZ sequence set with an odd integer L. If the following relation holds among N, M and L as*

$$N - (L-2) < ML \leq N + 1$$

then the new q-ary LCZ sequence set constructed by Construction 2.2.1 is also optimal in the sense that larger set cannot exist for given N, L and $\epsilon = 2$.

2.2.3 Examples

In this section we present two different LCZ sequence sets. The first example is taken from [21] which corresponds to the LCZ sequence set defined in Construction 2.2.1 with $(c_0, c_1) = (0, 2)$. The second example is produced similarly and it corresponds to the LCZ sequence set defined in Construction 2.2.1 with $(c_0, c_1) = (1, 3)$.

In the following examples we will use a LCZ sequence set V with parameters $(15, 3, 5, 1)$ given in [20]. Let $q = 4$, $n = 4$, $e = m = 2$ and α be a root of the primitive polynomial $x^4 + x + 1 \in \mathbb{F}_2[x]$. Define

$$V = \{v_i(t) | 0 \leq i \leq 2, \quad 0 \leq t \leq 14\}$$

where $v_i(t)$ is defined as

$$v_i(t) = \begin{cases} 2\mathrm{Tr}(\alpha^t) & \text{for } i = 0, \\ \mathrm{Tr}(\alpha^t) \oplus 2\mathrm{Tr}(\alpha^{t+5i}) & \text{otherwise.} \end{cases} \tag{2.16}$$

Note that $\oplus$ denotes the addition modulo 4 and Tr is the usual trace map from $\mathbb{F}_{2^4}$ to $\mathbb{F}_2$.

Then we see that V contains only the following sequences

$$\begin{aligned} v_1(t) &= [000200220202222], \\ v_2(t) &= [022120332301131], \\ v_3(t) &= [022320112103313]. \end{aligned}$$

Example 2.2.4 *[21, Example 12] Using Construction 2.2.1 with V as in (2.16) and* $(c_0, c_1) = (0, 2)$*, we obtain the following LCZ sequence set*

$$S_1 = \{s_i(t) | 0 \leq i \leq 5, \quad 0 \leq t \leq 29\}$$

where $s_i(t)$ *is given as*

$$\begin{aligned} s_0(t) &= [02000022020022200222020222202020], \\ s_1(t) &= [01222013230233302131031110321 2], \\ s_2(t) &= [03222031210211102313013330123 2], \\ s_3(t) &= [22202002222002002202220200000 0], \\ s_4(t) &= [21020033032213100111233130123 2], \\ s_5(t) &= [23020011012231300333211310321 2]. \end{aligned}$$

Note that according to the Tang, Fan, and Matsufuji bound (2.1) the above (30,6,5,2) LCZ sequence set is optimal, that is, larger set satisfying (2.1) does not exist with given $(N, L, \epsilon) = (30, 5, 2)$*. Clearly,*

$$ML - 1 = 6 * 5 - 1 = 29,$$

$$\frac{N(N-1)}{N-\epsilon^2} = \frac{30(30-1)}{30-2^2} \approx 33,$$

and

$$(M+1)L - 1 = (6+1) * 5 - 1 = 34.$$

Example 2.2.5 *Similarly, using Construction 2.2.1 with V as in (2.16) and* $(c_0, c_1) = (1, 3)$*, we obtain the following LCZ sequence set*

$$S_2 = \{s_i(t) | 0 \le i \le 5, \quad 0 \le t \le 29\}$$

where $s_i(t)$ *is given as*

$$\begin{aligned}
s_0(t) &= [12101032121032301232123230303 0], \\
s_1(t) &= [11323023331203003101132120022 2], \\
s_2(t) &= [13323001311221203323110300220 2], \\
s_3(t) &= [32303012323012103212321210101 0], \\
s_4(t) &= [31121003133223201121330100220 2], \\
s_5(t) &= [33121021113201001303312320022 2].
\end{aligned}$$

As in the case of previous example, this (30,6,5,2) LCZ sequence set is optimal with respect to the Tang, Fan, and Matsufuji bound (2.1).

Now we present the correlation distributions of the LCZ sequence sets given in Example 2.2.4 and Example 2.2.5 as follows:

Remark 2.2.6 *The LCZ sequence sets in Example 2.2.4 takes the correlation values in the set*

$$\{0, \pm 2, \pm 6, \pm 8, \pm 14, \pm 16, 30, \pm 16\omega, -2 \pm 16\omega, \pm 6 \pm 8\omega, \\ \pm 8 \pm 8\omega, \pm 14 \pm 8\omega, 14 \pm 16\omega, \pm 16 \pm 8\omega\}.$$

On the other hand the LCZ sequence sets in Example 2.2.5 takes the correlation values in the set

$$\{0, \pm 2, 14, \pm 16, 30, \pm 2\omega, \pm 6\omega, \pm 8\omega, \pm 14\omega, \pm 16\omega, -2 \pm 16\omega, \\ \pm 8 \pm 6\omega, \pm 8 \pm 8\omega, \pm 8 \pm 14\omega, 8 \pm 16\omega, 14 \pm 16\omega\}.$$

The above correlation values show that the obtained (30,6,5,2) LCZ sequence sets in Example 2.2.4 and Example 2.2.5 are different, since they have some different correlation values.

2.3 New class of quaternary LCZ sequence sets

In this section, we present a new class of quaternary LCZ sequence sets. We explicitly compute the full auto-correlations and cross-correlations of the sequences in these sets. We show that these new sequences are optimal with respect to the Tang, Fan and Matsufiji (2.1) bound.

This section is organized as follows. In Section 2.3.1 we fix some notations and give some useful technical results. In Section 2.3.2 we present two quaternary LCZ sequence set $\mathcal{S}_1$ and $\mathcal{S}_2$ and we compute the correlation distributions of the sequences in these sets. Finally in Section 2.3.3 we present the constructions of optimal quaternary LCZ sequence sets.

2.3.1 Preliminaries and Some Technical Results

In this part we give some notations and a useful lemma which will be used for computing the correlation distributions of the sequences presented in this section.

Let n be a positive integer. Recall that Tr is the trace map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Let φ be the embedding of $\mathbb{F}_2$ into $\mathbb{Z}_4$ defined as

$$\begin{array}{rcl} \varphi : \mathbb{F}_2 & \hookrightarrow & \mathbb{Z}_4 \\ x & \mapsto & x, \end{array}$$

that is, $\varphi(0) = 0$ and $\varphi(1) = 1$. Now using this embedding let us define tr as

$$\begin{array}{rcl} \mathrm{tr} : \mathbb{F}_{2^n} & \hookrightarrow & \mathbb{Z}_4 \\ x & \mapsto & \varphi(\mathrm{Tr}(x)). \end{array} \tag{2.17}$$

Throughout the rest of this section we assume that $\omega = \sqrt{-1}$.

We start with a crucial lemma. It will be used in the proof of Theorem 2.3.3, Theorem 2.3.5 and Theorem 2.3.7.

Lemma 2.3.1 *Let $a, b \in \mathbb{F}_{2^n}^*$ and assume that $a \neq b$, $a \neq 1$ and $b \neq 1$. Then we have the following identities.*

$$\textbf{1}. \quad \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{\mathrm{tr}(x)} = 2^{n-1} - 1 + 2^{n-1}\omega, \tag{2.18}$$

$$\textbf{2}. \quad \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{3\mathrm{tr}(x)} = 2^{n-1} - 1 - 2^{n-1}\omega, \tag{2.19}$$

$$\textbf{3}. \quad \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{\mathrm{tr}(x)+2\mathrm{tr}(ax)} = -1 \tag{2.20}$$

$$\textbf{4}. \quad \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{\mathrm{tr}(x)+3\mathrm{tr}(ax)} = 2^{n-1} - 1, \tag{2.21}$$

$$\textbf{5}. \quad \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{\mathrm{tr}(x)+\mathrm{tr}(ax)} = -1 + 2^{n-1}\omega, \tag{2.22}$$

$$\textbf{6}. \quad \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{2\mathrm{tr}(x)+2\mathrm{tr}(ax)} = -1, \tag{2.23}$$

$$\textbf{7}. \quad \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{3\mathrm{tr}(x)+3\mathrm{tr}(ax)} = -1 - 2^{n-1}\omega, \tag{2.24}$$

$$\textbf{8}. \quad \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{\mathrm{tr}(x)+\mathrm{tr}(ax)+2\mathrm{tr}(bx)} = \begin{cases} -1 - 2^{n-1}\omega, & \text{if } b = a+1 \\ -1, & \text{otherwise,} \end{cases} \tag{2.25}$$

$$\textbf{9}. \quad \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{3\mathrm{tr}(x)+3\mathrm{tr}(ax)+2\mathrm{tr}(bx)} = \begin{cases} -1 + 2^{n-1}\omega, & \text{if } b = a+1 \\ -1, & \text{otherwise.} \end{cases} \tag{2.26}$$

Proof. First we observe that for any

$$f(x) : \mathbb{F}_{2^n}^* \to \mathbb{Z}_4,$$

if we denote

$$N_i = |\{x \in \mathbb{F}_{2^n}^* : f(x) = i\}|, \quad \text{for } i \in \mathbb{Z}_4,$$

then it follows immediately that,

$$\sum_{x \in \mathbb{F}_{2^n}^*} \omega^{f(x)} = (N_0 - N_2) + (N_1 - N_3)\omega. \tag{2.27}$$

Moreover we know that, for any $\alpha \in \mathbb{F}_{2^n}^*$, $\mathrm{Tr}(\alpha x)$ is a balanced linear Boolean function on $\mathbb{F}_{2^n}$, that is,

$$|\{x \in \mathbb{F}_{2^n} : \mathrm{Tr}(\alpha x) = 0\}| = |\{x \in \mathbb{F}_{2^n} : \mathrm{Tr}(\alpha x) = 1\}| = 2^{n-1}, \tag{2.28}$$

and note that $\mathrm{Tr}(0) = 0$.

Now (2.18) and (2.19) follows immediately using (2.17), (2.27) and (2.28).

Furthermore, we know that for any $\alpha_1, \alpha_2 \in \mathbb{F}_{2^n}^*$, $\mathrm{Tr}(\alpha_1 x)$ and $\mathrm{Tr}(\alpha_2 x)$ are orthogonal linear Boolean function on $\mathbb{F}_{2^n}$, that is,

$$\begin{aligned} |\{x \in \mathbb{F}_{2^n} : \mathrm{Tr}(\alpha_1 x) = \mathrm{Tr}(\alpha_2 x) = 0\}| &= 2^{n-2}, \\ |\{x \in \mathbb{F}_{2^n} : \mathrm{Tr}(\alpha_1 x) = \mathrm{Tr}(\alpha_2 x) = 1\}| &= 2^{n-2}, \\ |\{x \in \mathbb{F}_{2^n} : \mathrm{Tr}(\alpha_1 x) = 0,\ \mathrm{Tr}(\alpha_2 x) = 1\}| &= 2^{n-2}, \\ |\{x \in \mathbb{F}_{2^n} : \mathrm{Tr}(\alpha_1 x) = 1,\ \mathrm{Tr}(\alpha_2 x) = 0\}| &= 2^{n-2}. \end{aligned} \tag{2.29}$$

Now using (2.17), (2.27) and (2.29) we obtain (2.20), (2.21), (2.22), (2.23) and (2.24).

Lastly we obtain the last two equations using the orthogonality of linear Boolean functions, (2.17) and the following observations

$$\mathrm{tr}(x) + \mathrm{tr}(ax) + 2\mathrm{tr}(bx) = \begin{cases} \mathrm{tr}((1+a)x) + 2\mathrm{tr}(bx), & \text{if } \mathrm{tr}(x)\mathrm{tr}(ax) \neq 1, \\ 2 + 2\mathrm{tr}(bx) & \text{if } \mathrm{tr}(x)\mathrm{tr}(ax) = 1, \end{cases}$$

$$3\mathrm{tr}(x) + 3\mathrm{tr}(ax) + 2\mathrm{tr}(bx) = \begin{cases} 3\mathrm{tr}((1+a)x) + 2\mathrm{tr}(bx), & \text{if } \mathrm{tr}(x)\mathrm{tr}(ax) \neq 1, \\ 2 + 2\mathrm{tr}(bx) & \text{if } \mathrm{tr}(x)\mathrm{tr}(ax) = 1. \end{cases}$$

■

2.3.2 Quaternary LCZ sequence sets $\mathcal{S}_1$ and $\mathcal{S}_2$

In this section, we construct quaternary LCZ sequence sets $\mathcal{S}_1$ and $\mathcal{S}_2$. Also we compute the correlation distribution of the sequences in the sets $\mathcal{S}_1$ and $\mathcal{S}_2$. The definition of the set $\mathcal{S}_1$ is as follows:

Definition 2.3.2 *Let e, n be positive integers such that $e|n$ and let α and θ be primitive elements of $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^e}$, respectively.*

Let $\mathcal{S}_1$ be the sequence set

$$\mathcal{S}_1 = \{s_i(t) | 0 \leq t \leq 2(2^n - 1) - 1,\ 0 \leq i \leq 2^e - 2\},$$

where

$$s_0(t) = \begin{cases} 2\mathrm{tr}\left(\alpha^{t_1}\right), & \text{if } t = 2t_1 \\ 2\mathrm{tr}\left(\alpha^{t_1+2^{n-1}}\right), & \text{if } t = 2t_1 + 1, \end{cases}$$

and for $1 \le i \le 2^e - 2$

$$s_i(t) = \begin{cases} \mathrm{tr}\left(\alpha^{t_1}\right) + 2\mathrm{tr}\left(\alpha^{t_1}\theta^i\right), & \text{if } t = 2t_1 \\ 3\mathrm{tr}\left(\alpha^{t_1+2^{n-1}}\right) + 2\mathrm{tr}\left(\alpha^{t_1+2^{n-1}}\theta^i\right), & \text{if } t = 2t_1 + 1. \end{cases}$$

In the following theorem we compute the correlation distribution of the sequences in the set $\mathcal{S}_1$.

Theorem 2.3.3 *Let* $s_i(t), s_j(t) \in \mathcal{S}_1$ *be two arbitrary sequences and* $0 \le \tau \le 2^{n+1} - 3$ *be an integer. Let* α *and* θ *be primitive elements of* $\mathbb{F}_{2^n}$ *and* $\mathbb{F}_{2^e}$*, respectively. Set* $a = \theta^i$*,* $b = \theta^j$*,* $\beta = \alpha^{\lfloor \frac{\tau}{2} \rfloor}$ *and* $\delta = \alpha^{2^{n-1}}$*, where* $\left\lfloor \frac{\tau}{2} \right\rfloor$ *is the greatest integer less than* $\frac{\tau}{2}$*. Then the correlation distribution of the sequences in the set* $\mathcal{S}_1$ *is as follows:*

If $\tau = 2\tau_1$*, then*

$$R_{i,j}(\tau) = \begin{cases} 2(2^n - 1), & \text{if } i = j \text{ and } \beta = 1 \\ 2^n - 2, & \text{if } i \neq 0, j = 0 \text{ and } (\beta = a \text{ or } \beta = a + 1) \\ 2^n - 2, & \text{if } i = 0, j \neq 0 \text{ and } \left(\beta = \dfrac{1}{b} \text{ or } \beta = \dfrac{1}{b+1}\right) \\ 2^n - 2, & \text{if } i \neq j,\ i \cdot j \neq 0 \text{ and } \left(\beta = \dfrac{a}{b} \text{ or } \beta = \dfrac{a+1}{b+1}\right) \\ -2, & \text{otherwise}. \end{cases}$$

If $\tau = 2\tau_1 + 1$, *then*

$$R_{i,j}(\tau) = \begin{cases} 2(2^n - 1), & \text{if } i = j = 0 \text{ and } \beta = \dfrac{1}{\delta} \\ 2^n - 2, & \text{if } i = j \neq 0 \text{ and } \left(\beta = \dfrac{a}{\delta(a+1)} \text{ or } \beta = \dfrac{a+1}{\delta a}\right) \\ 2^n - 2, & \text{if } i \neq 0, j = 0 \text{ and } \left(\beta = \dfrac{a}{\delta} \text{ or } \beta = \dfrac{a+1}{\delta}\right) \\ 2^n - 2, & \text{if } i = 0, j \neq 0 \text{ and } \left(\beta = \dfrac{1}{\delta b} \text{ or } \beta = \dfrac{1}{\delta(b+1)}\right) \\ 2^n - 2, & \text{if } i \neq j,\ i \cdot j \neq 0 \text{ and } \left(\beta = \dfrac{a}{\delta(b+1)} \text{ or } \beta = \dfrac{a+1}{\delta b}\right) \\ -2, & \text{otherwise.} \end{cases}$$

Proof. In the first part of the proof we compute the correlation function $R_{i,j}(\tau)$ of sequences $s_i(t), s_j(t) \in \mathcal{S}_1$ when τ is an even integer with $\tau = 2\tau_1$.

Similar to the (2.7), $R_{i,j}(\tau)$ can be written as

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{2^{n+1}-3} \omega^{s_i(t) - s_j(t+\tau)} \\ &= \sum_{t=0}^{2^n-2} \omega^{s_i(2t) - s_j(2t+\tau)} + \sum_{t=0}^{2^n-2} \omega^{s_i(2t+1) - s_j(2t+1+\tau)} \\ &= \sum_{t=0}^{2^n-2} \omega^{s_i(2t) - s_j(2(t+\tau_1))} + \sum_{t=0}^{2^n-2} \omega^{s_i(2t+1) - s_j(2(t+\tau_1)+1)}. \end{aligned} \tag{2.30}$$

Now we must consider the following five cases separately.

Case 1. $i = j = 0$.

In this case, $R_{i,j}(\tau)$ in (2.30) becomes,

$$\begin{aligned} R_{0,0}(\tau) &= \sum_{t=0}^{2^n-2} \omega^{2\mathrm{tr}(\alpha^t) - 2\mathrm{tr}(\alpha^{t+\tau_1})} + \sum_{t=0}^{2^n-2} \omega^{2\mathrm{tr}\left(\alpha^{t+2^{n-1}}\right) - 2\mathrm{tr}\left(\alpha^{t+\tau_1+2^{n-1}}\right)} \\ &= \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{2\mathrm{tr}(x) - 2\mathrm{tr}(\beta x)} + \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{2\mathrm{tr}(x\delta) - 2\mathrm{tr}(\beta x \delta)} \\ &= \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{2\mathrm{tr}(x) + 2\mathrm{tr}(\beta x)} + \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{2\mathrm{tr}(x) + 2\mathrm{tr}(\beta x)}. \end{aligned} \tag{2.31}$$

Here we note that if x runs through $\mathbb{F}_{2^n}^*$ then δx runs through $\mathbb{F}_{2^n}^*$, since $\delta = \alpha^{2^{n-1}}$ is also a primitive element in $\mathbb{F}_{2^n}^*$ as $gcd(2^{n-1}, 2^n - 1) = 1$. We will use this property in all of the below cases. Also we use the addition property in $\mathbb{Z}_4$, that is, we use the equality

$$2\mathrm{tr}(x) - 2\mathrm{tr}(\beta x) = 2\mathrm{tr}(x) + 2\mathrm{tr}(\beta x) \text{ in } \mathbb{Z}_4.$$

Now if $\beta = 1$, then $2\mathrm{tr}(\beta x) + 2\mathrm{tr}(x) = 0$ for all $x \in \mathbb{F}_{2^n}^*$. Hence using (2.31), we obtain

$$R_{0,0}(\tau) = (2^n - 1) + (2^n - 1) = 2(2^n - 1).$$

If $\beta \neq 1$, then using (2.23) and (2.31), we have

$$R_{0,0}(\tau) = (-1) + (-1) = -2.$$

Case 2. $i = j \neq 0$.

In this case, $R_{i,j}(\tau)$ in (2.30) becomes,

$$\begin{aligned} R_{i,i}(\tau) &= \sum_{t=0}^{2^n-2} \omega^{\mathrm{tr}(\alpha^t)+2\mathrm{tr}(\alpha^t\theta^i)-\mathrm{tr}(\alpha^{t+\tau_1})-2\mathrm{tr}(\alpha^{t+\tau_1}\theta^i)} \\ &\quad + \sum_{t=0}^{2^n-2} \omega^{3\mathrm{tr}\left(\alpha^{t+2^{n-1}}\right)+2\mathrm{tr}\left(\alpha^{t+2^{n-1}}\theta^i\right)-3\mathrm{tr}\left(\alpha^{t+\tau_1+2^{n-1}}\right)-2\mathrm{tr}\left(\alpha^{t+\tau_1+2^{n-1}}\theta^i\right)} \\ &= \sum_{x\in\mathbb{F}_{2^n}^*} \omega^{\mathrm{tr}(x)+3\mathrm{tr}(\beta x)+2\mathrm{tr}\left(x\left(\theta^i+\beta\theta^i\right)\right)} + \sum_{x\in\mathbb{F}_{2^n}^*} \omega^{3\mathrm{tr}(x)+\mathrm{tr}(\beta x)+2\mathrm{tr}\left(x\left(\theta^i+\beta\theta^i\right)\right)}. \quad (2.32) \end{aligned}$$

Now if $\beta = 1$, then

$$\mathrm{tr}(x) + 3\mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^i\right)\right) = 3\mathrm{tr}(x) + \mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^i\right)\right) = 0$$

for all $x \in \mathbb{F}_{2^n}^*$. Hence using (2.32), we obtain

$$R_{i,i}(\tau) = (2^n - 1) + (2^n - 1) = 2(2^n - 1).$$

If $\beta = \dfrac{\theta^i}{\theta^i + 1}$, then

$$\mathrm{tr}(x) + 3\mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^i\right)\right) = \mathrm{tr}(x) + \mathrm{tr}(\beta x),$$

and

$$3\mathrm{tr}(x) + \mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^i\right)\right) = 3\mathrm{tr}(x) + 3\mathrm{tr}(\beta x).$$

Similarly, if $\beta = \dfrac{\theta^i + 1}{\theta^i}$, then

$$\mathrm{tr}(x) + 3\mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^i\right)\right) = 3\mathrm{tr}(x) + 3\mathrm{tr}(\beta x),$$

and

$$3\mathrm{tr}(x) + \mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^i\right)\right) = \mathrm{tr}(x) + \mathrm{tr}(\beta x).$$

Now using (2.22), (2.24) and (2.32), we obtain that

$$R_{i,i}(\tau) = \left(-1 - 2^{n-1}\omega\right) + \left(-1 + 2^{n-1}\omega\right) = -2,$$

when $\beta \in \left\{\dfrac{\theta^i}{\theta^i+1}, \dfrac{\theta^i+1}{\theta^i}\right\}$.

Lastly, if $\beta \notin \left\{1, \dfrac{\theta^i}{\theta^i+1}, \dfrac{\theta^i+1}{\theta^i}\right\}$, then observing

$$\begin{aligned}
\mathrm{tr}(\beta x) + 3\mathrm{tr}(x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^i\right)\right) &= 3\mathrm{tr}(\beta x) + 3\mathrm{tr}(x) + 2\mathrm{tr}\left(x\left(\beta + \theta^i + \beta\theta^i\right)\right), \\
3\mathrm{tr}(\beta x) + \mathrm{tr}(x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^i\right)\right), &= \mathrm{tr}(\beta x) + \mathrm{tr}(x) + 2\mathrm{tr}\left(x\left(\beta + \theta^i + \beta\theta^i\right)\right)
\end{aligned}$$

and using (2.25), (2.26) and (2.32), we obtain

$$R_{i,i}(\tau) = (-1) + (-1) = -2.$$

Case 3. $i \neq 0$ and $j = 0$.

In this case, $R_{i,j}(\tau)$ in (2.30) becomes,

$$\begin{aligned}
R_{i,0}(\tau) &= \sum_{t=0}^{2^n-2} \omega^{\mathrm{tr}(\alpha^t)+2\mathrm{tr}(\alpha^t\theta^i)-2\mathrm{tr}(\alpha^{t+\tau_1})} \\
&\quad + \sum_{t=0}^{2^n-2} \omega^{3\mathrm{tr}\left(\alpha^{t+2^{n-1}}\right)+2\mathrm{tr}\left(\alpha^{t+2^{n-1}}\theta^i\right)-2\mathrm{tr}\left(\alpha^{t+\tau_1+2^{n-1}}\right)} \\
&= \sum_{x\in\mathbb{F}_{2^n}^*} \omega^{\mathrm{tr}(x)+2\mathrm{tr}\left(x\left(\theta^i+\beta\right)\right)} + \sum_{x\in\mathbb{F}_{2^n}^*} \omega^{3\mathrm{tr}(x)+2\mathrm{tr}\left(x\left(\theta^i+\beta\right)\right)}. \qquad (2.33)
\end{aligned}$$

Now if $\beta \in \left\{\theta^i, \theta^i + 1\right\}$, then using (2.18), (2.19) and (2.33), we obtain

$$R_{i,0}(\tau) = \left(2^{n-1} - 1 + 2^{n-1}\omega\right) + \left(2^{n-1} - 1 - 2^{n-1}\omega\right) = 2^n - 2.$$

Moreover if $\beta \notin \left\{\theta^i, \theta^i + 1\right\}$, then observing

$$3\mathrm{tr}(x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\right)\right) = \mathrm{tr}(x) + 2\mathrm{tr}\left(x\left(1 + \theta^i + \beta\right)\right),$$

and using (2.20) and (2.33), we obtain

$$R_{i,0}(\tau) = (-1) + (-1) = -2.$$

Case 4. $i = 0$ and $j \neq 0$.

In this case, $R_{i,j}(\tau)$ in (2.30) becomes,

$$\begin{aligned} R_{0,j}(\tau) &= \sum_{t=0}^{2^n-2} \omega^{2\mathrm{tr}\left(\alpha^t\right)-\mathrm{tr}\left(\alpha^{t+\tau_1}\right)-2\mathrm{tr}\left(\alpha^{t+\tau_1}\theta^j\right)} \\ &\quad + \sum_{t=0}^{2^n-2} \omega^{2\mathrm{tr}\left(\alpha^{t+2^{n-1}}\right)-3\mathrm{tr}\left(\alpha^{t+\tau_1+2^{n-1}}\right)-2\mathrm{tr}\left(\alpha^{t+\tau_1+2^{n-1}}\theta^j\right)} \\ &= \sum_{x\in\mathbb{F}_{2^n}^*} \omega^{3\mathrm{tr}(\beta x)+2\mathrm{tr}\left(x\left(1+\beta\theta^j\right)\right)} + \sum_{x\in\mathbb{F}_{2^n}^*} \omega^{\mathrm{tr}(\beta x)+2\mathrm{tr}\left(x\left(1+\beta\theta^j\right)\right)}. \end{aligned} \tag{2.34}$$

Similar to the Case 3, using (2.18), (2.19), (2.20) and (2.34), we obtain

$$R_{0,j}(\tau) = \begin{cases} 2^n-2, & \text{if } \beta \in \left\{\frac{1}{\theta^j}, \frac{1}{\theta^j+1}\right\} \\ -2, & \text{otherwise,} \end{cases}$$

Case 5. $i \neq j$, $i \neq 0$ and $j \neq 0$.

In this case, $R_{i,j}(\tau)$ in (2.30) becomes,

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{2^n-2} \omega^{\mathrm{tr}\left(\alpha^t\right)+2\mathrm{tr}\left(\alpha^t\theta^i\right)-\mathrm{tr}\left(\alpha^{t+\tau_1}\right)-2\mathrm{tr}\left(\alpha^{t+\tau_1}\theta^j\right)} \\ &\quad + \sum_{t=0}^{2^n-2} \omega^{3\mathrm{tr}\left(\alpha^{t+2^{n-1}}\right)+2\mathrm{tr}\left(\alpha^{t+2^{n-1}}\theta^i\right)-3\mathrm{tr}\left(\alpha^{t+\tau_1+2^{n-1}}\right)-2\mathrm{tr}\left(\alpha^{t+\tau_1+2^{n-1}}\theta^j\right)} \\ &= \sum_{x\in\mathbb{F}_{2^n}^*} \omega^{\mathrm{tr}(x)+3\mathrm{tr}(\beta x)+2\mathrm{tr}\left(x\left(\theta^i+\beta\theta^j\right)\right)} + \sum_{x\in\mathbb{F}_{2^n}^*} \omega^{3\mathrm{tr}(x)+\mathrm{tr}(\beta x)+2\mathrm{tr}\left(x\left(\theta^i+\beta\theta^j\right)\right)}. \end{aligned} \tag{2.35}$$

Now if $\beta = 1$, then

$$\mathrm{tr}(x) + 3\mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i+\beta\theta^j\right)\right) = 3\mathrm{tr}(x) + \mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i+\beta\theta^j\right)\right) = 2\mathrm{tr}\left(x\left(\theta^i+\theta^j\right)\right)$$

for all $x \in \mathbb{F}_{2^n}^*$. Hence using (2.35), we obtain

$$R_{i,j}(\tau) = (-1) + (-1) = -2.$$

If $\beta = \dfrac{\theta^i}{\theta^j}$, then

$$\mathrm{tr}(x) + 3\mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i+\beta\theta^j\right)\right) = \mathrm{tr}(x) + 3\mathrm{tr}(\beta x),$$

and

$$3\mathrm{tr}(x) + \mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i+\beta\theta^j\right)\right) = 3\mathrm{tr}(x) + \mathrm{tr}(\beta x).$$

Similarly, if $\beta = \dfrac{1+\theta^i}{1+\theta^j}$, then

$$\mathrm{tr}(x) + 3\mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^j\right)\right) = 3\mathrm{tr}(x) + \mathrm{tr}(\beta x),$$

and

$$3\mathrm{tr}(x) + \mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^j\right)\right) = \mathrm{tr}(x) + 3\mathrm{tr}(\beta x).$$

Now using (2.21) and (2.35), we obtain that

$$R_{i,j}(\tau) = \left(2^{n-1} - 1\right) + \left(2^{n-1} - 1\right) = 2^n - 2,$$

when $\beta \in \left\{\dfrac{\theta^i}{\theta^j}, \dfrac{1+\theta^i}{1+\theta^j}\right\}$.

If $\beta = \dfrac{\theta^i}{\theta^j + 1}$, then

$$\mathrm{tr}(x) + 3\mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^j\right)\right) = \mathrm{tr}(x) + \mathrm{tr}(\beta x),$$

and

$$3\mathrm{tr}(x) + \mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^j\right)\right) = 3\mathrm{tr}(x) + 3\mathrm{tr}(\beta x).$$

Similarly, if $\beta = \dfrac{\theta^i + 1}{\theta^j}$, then

$$\mathrm{tr}(x) + 3\mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^j\right)\right) = 3\mathrm{tr}(x) + 3\mathrm{tr}(\beta x),$$

and

$$3\mathrm{tr}(x) + \mathrm{tr}(\beta x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^j\right)\right) = \mathrm{tr}(x) + \mathrm{tr}(\beta x).$$

Now using (2.22), (2.24) and (2.35), we obtain that

$$R_{i,j}(\tau) = \left(-1 - 2^{n-1}\omega\right) + \left(-1 + 2^{n-1}\omega\right) = -2,$$

when $\beta \in \left\{\dfrac{\theta^i}{\theta^j + 1}, \dfrac{\theta^i + 1}{\theta^j}\right\}$.

Lastly, if $\beta \notin \left\{1, \dfrac{\theta^i}{\theta^j}, \dfrac{1+\theta^i}{1+\theta^j}, \dfrac{\theta^i}{\theta^j+1}, \dfrac{\theta^i+1}{\theta^j}\right\}$, then observing

$$\begin{aligned}
\mathrm{tr}(\beta x) + 3\mathrm{tr}(x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^j\right)\right) &= 3\mathrm{tr}(\beta x) + 3\mathrm{tr}(x) + 2\mathrm{tr}\left(x\left(\beta + \theta^i + \beta\theta^j\right)\right), \\
3\mathrm{tr}(\beta x) + \mathrm{tr}(x) + 2\mathrm{tr}\left(x\left(\theta^i + \beta\theta^j\right)\right) &= \mathrm{tr}(\beta x) + \mathrm{tr}(x) + 2\mathrm{tr}\left(x\left(\beta + \theta^i + \beta\theta^j\right)\right),
\end{aligned}$$

and using (2.25), (2.26) and (2.35), we obtain

$$R_{i,j}(\tau) = (-1) + (-1) = -2.$$

This completes the proof of theorem for τ is even.

In the second part of the proof we assume that τ is odd, that is, $\tau = 2\tau_1 + 1$ for some integer τ_1. Similar to the first part of the proof, by considering the same 5 cases we obtain the desired results.

■

Now we will give the definition of the set $\mathcal{S}_2$ as follows.

Definition 2.3.4 *Let e, n be positive integers such that $e|n$, and let α and θ be primitive elements of $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^e}$, respectively.*

Let $\mathcal{S}_2$ be the sequence set

$$\mathcal{S}_2 = \{s_i(t) | 0 \leq t \leq 2(2^n - 1) - 1,\ 2^e - 1 \leq i \leq 2^{e+1} - 3\},$$

where

$$s_{2^e-1}(t) = \begin{cases} 2\mathrm{tr}\left(\alpha^{t_1}\right) + 2, & t = 2t_1 \\ 2\mathrm{tr}\left(\alpha^{t_1+2^{n-1}}\right), & t = 2t_1 + 1, \end{cases}$$

and for $2^e \leq i \leq 2^{e+1} - 3$

$$s_i(t) = \begin{cases} \mathrm{tr}\left(\alpha^{t_1}\right) + 2\mathrm{tr}\left(\alpha^{t_1}\theta^i\right) + 2, & t = 2t_1 \\ 3\mathrm{tr}\left(\alpha^{t_1+2^{n-1}}\right) + 2\mathrm{tr}\left(\alpha^{t_1+2^{n-1}}\theta^i\right), & t = 2t_1 + 1. \end{cases}$$

The following theorem gives the correlation distribution of the sequences in the set $\mathcal{S}_2$.

Theorem 2.3.5 *Let $s_i(t), s_j(t) \in \mathcal{S}_2$ be two arbitrary sequences and $0 \leq \tau \leq 2^{n+1} - 3$ be an integer. Let α and θ be primitive elements of $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^e}$, respectively. Set $a = \theta^i$, $b = \theta^j$, $\beta = \alpha^{\lfloor \frac{\tau}{2} \rfloor}$ and $\delta = \alpha^{2^{n-1}}$. Then the correlation distribution of the sequences in the set $\mathcal{S}_2$ is as follows:*

If $\tau = 2\tau_1$, *then*

$$R_{i,j}(\tau) = \begin{cases} 2(2^n - 1), & \text{if } i = j \text{ and } \beta = 1 \\ 2^n - 2, & \text{if } i \neq 0,\ j = 0 \text{ and } (\beta = a \text{ or } \beta = a + 1) \\ 2^n - 2, & \text{if } i = 0,\ j \neq 0 \text{ and } \left(\beta = \dfrac{1}{b} \text{ or } \beta = \dfrac{1}{b+1}\right) \\ 2^n - 2, & \text{if } i \neq j,\ i \cdot j \neq 0 \text{ and } \left(\beta = \dfrac{a}{b} \text{ or } \beta = \dfrac{a+1}{b+1}\right) \\ -2, & \text{otherwise.} \end{cases}$$

If $\tau = 2\tau_1 + 1$, *then*

$$R_{i,j}(\tau) = \begin{cases} -2(2^n - 1), & \text{if } i = j = 0 \text{ and } \beta = \dfrac{1}{\delta} \\ -2^n + 2, & \text{if } i = j \neq 0 \text{ and } \left(\beta = \dfrac{a}{\delta(a+1)} \text{ or } \beta = \dfrac{a+1}{\delta a}\right) \\ -2^n + 2, & \text{if } i \neq 0,\ j = 0 \text{ and } \left(\beta = \dfrac{a}{\delta} \text{ or } \beta = \dfrac{a+1}{\delta}\right) \\ -2^n + 2, & \text{if } i = 0,\ j \neq 0 \text{ and } \left(\beta = \dfrac{1}{\delta b} \text{ or } \beta = \dfrac{1}{\delta(b+1)}\right) \\ -2^n + 2, & \text{if } i \neq j,\ i \cdot j \neq 0 \text{ and } \left(\beta = \dfrac{a}{\delta(b+1)} \text{ or } \beta = \dfrac{a+1}{\delta b}\right) \\ 2, & \text{otherwise.} \end{cases}$$

Proof. Similar to the (2.7), $R_{i,j}(\tau)$ can be written as

$$\begin{aligned}
R_{i,j}(\tau) &= \sum_{t=0}^{2^{n+1}-3} \omega^{s_i(t)-s_j(t+\tau)} \\
&= \sum_{t=0}^{2^n-2} \omega^{s_i(2t)-s_j(2t+\tau)} + \sum_{t=0}^{2^n-2} \omega^{s_i(2t+1)-s_j(2t+1+\tau)} \\
&= \begin{cases} \sum_{t=0}^{2^n-2} \omega^{s_i(2t)-s_j(2(t+\tau_1))} + \sum_{t=0}^{2^n-2} \omega^{s_i(2t+1)-s_j(2(t+\tau_1)+1)} & \text{if } \tau = 2\tau_1 \\ \sum_{t=0}^{2^n-2} \omega^{s_i(2t)-s_j(2(t+\tau_1)+1)} + \sum_{t=0}^{2^n-2} \omega^{s_i(2t+1)-s_j(2(t+\tau_1)+2)} & \text{if } \tau = 2\tau_1+1 \end{cases} \\
&= \begin{cases} \sum_{t=0}^{2^n-2} \omega^{s_{i-(2^e-1)}(2t)+2-s_{j-(2^e-1)}(2(t+\tau_1))-2} \\ \quad + \sum_{t=0}^{2^n-2} \omega^{s_{i-(2^e-1)}(2t+1)-s_{j-(2^e-1)}(2(t+\tau_1)+1)} & \text{if } \tau = 2\tau_1 \\ \sum_{t=0}^{2^n-2} \omega^{s_{i-(2^e-1)}(2t)+2-s_{j-(2^e-1)}(2(t+\tau_1)+1)} \\ \quad + \sum_{t=0}^{2^n-2} \omega^{s_{i-(2^e-1)}(2t+1)-s_{j-(2^e-1)}(2(t+\tau_1)+2)-2} & \text{if } \tau = 2\tau_1+1 \end{cases} \\
&= \begin{cases} R_{i-(2^e-1),j-(2^e-1)}(\tau) \text{ if } \tau = 2\tau_1 \\ -R_{i-(2^e-1),j-(2^e-1)}(\tau) \text{ if } \tau = 2\tau_1+1. \end{cases}
\end{aligned}$$

We complete the proof by using Theorem 2.3.3. ■

Now immediately we have the following result.

Theorem 2.3.6 *The sets $\mathcal{S}_1$ and $\mathcal{S}_2$ are quaternary LCZ sequence sets with parameters*

$$\left(2(2^n-1), (2^e-1), \frac{2^n-1}{2^e-1}, 2\right).$$

Proof. Let α be a primitive element of $\mathbb{F}_{2^n}$ and $\beta = \alpha^{\lfloor \frac{\tau}{2} \rfloor}$ and $\delta = \alpha^{2^{n-1}} = \alpha^{\frac{1}{2}}$. Then we have

$$\alpha^{\frac{\tau}{2}} = \begin{cases} \beta \text{ if } \tau \text{ is even} \\ \delta\beta \text{ if } \tau \text{ is odd.} \end{cases} \tag{2.36}$$

Now $\alpha^{\frac{\tau}{2}} \in \mathbb{F}_{2^e}$ if and only if $2^n - 1 \left| \frac{\tau}{2}(2^e-1) \right.$, which means

$$\frac{2^n-1}{2^e-1} \Big| \tau,$$

as $\gcd(2, 2^n-1) = 1$ and $2^e - 1 | 2^n - 1$. Therefore,

$$\alpha^{\frac{\tau}{2}} \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^e} \quad \text{if} \quad |\tau| < \frac{2^n-1}{2^e-1} \quad \text{and} \quad \alpha^{\frac{\tau}{2}} \in \mathbb{F}_{2^e} \quad \text{if} \quad |\tau| = \frac{2^n-1}{2^e-1}.$$

We complete the proof using the correlation distributions in Theorem 2.3.3, Theorem 2.3.5, the Definition 2.1.2 of LCZ sequence set and (2.36). ■

Similar to the Theorem 2.3.3 and Theorem 2.3.5 we compute the correlation distribution of the sequences taken from different sets $\mathcal{S}_1$ and $\mathcal{S}_2$ in the following theorem.

Theorem 2.3.7 *Let $s_i(t) \in \mathcal{S}_1$ and $s_j(t) \in \mathcal{S}_2$ be two arbitrary sequences and $0 \leq \tau \leq 2^{n+1}-3$ be an integer. Let α and θ be primitive elements of $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^e}$, respectively. Set $a = \theta^i$, $b = \theta^j$, $\beta = \alpha^{\lfloor \frac{\tau}{2} \rfloor}$ and $\delta = \alpha^{2^{n-1}}$. Then the correlation distribution of the sequences $s_i(t)$ and $s_j(t)$ is as follows:*

If $\tau = 2\tau_1$, then

$$R_{i,j}(\tau) = R_{j,i}(\tau) = \begin{cases} 2^n\omega, & \text{if } i = j \neq 0 \text{ and } \beta = \dfrac{a+1}{a} \\ -2^n\omega, & \text{if } i = j \neq 0 \text{ and } \beta = \dfrac{a}{a+1} \\ 2^n\omega, & \text{if } i \neq 0, j = 0 \text{ and } \beta = a+1 \\ -2^n\omega, & \text{if } i \neq 0, j = 0 \text{ and } \beta = a \\ 2^n\omega, & \text{if } i = 0, j \neq 0 \text{ and } \beta = \dfrac{1}{b} \\ -2^n\omega, & \text{if } i = 0, j \neq 0 \text{ and } \beta = \dfrac{1}{b+1} \\ 2^n\omega, & \text{if } i \neq j,\ i \cdot j \neq 0 \text{ and } \beta = \dfrac{a+1}{b} \\ -2^n\omega, & \text{if } i \neq j,\ i \cdot j \neq 0 \text{ and } \beta = \dfrac{a}{b+1} \\ 0, & \text{otherwise.} \end{cases}$$

If $\tau = 2\tau_1 + 1$, *then*

$$R_{i,j}(\tau) = -R_{j,i}(\tau) = \begin{cases} -2^n\omega, & \text{if } i \neq 0, j = 0 \text{ and } \beta = \dfrac{a+1}{\delta} \\ 2^n\omega, & \text{if } i \neq 0, j = 0 \text{ and } \beta = \dfrac{a}{\delta} \\ -2^n\omega, & \text{if } i = 0, j \neq 0 \text{ and } \beta = \dfrac{1}{\delta(b+1)} \\ 2^n\omega, & \text{if } i = 0, j \neq 0 \text{ and } \beta = \dfrac{1}{\delta b} \\ -2^n\omega, & \text{if } i \neq j,\ i \cdot j \neq 0 \text{ and } \beta = \dfrac{a+1}{\delta(b+1)} \\ 2^n\omega, & \text{if } i \neq j,\ i \cdot j \neq 0 \text{ and } \beta = \dfrac{a}{\delta b} \\ 0, & \text{otherwise}. \end{cases}$$

Proof. Similar to the proof of Theorem 2.3.5, $R_{i,j}(\tau)$ can be written as

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{2^{n+1}-3} \omega^{s_i(t)-s_j(t+\tau)} \\ &= \sum_{t=0}^{2^n-2} \omega^{s_i(2t)-s_j(2t+\tau)} + \sum_{t=0}^{2^n-2} \omega^{s_i(2t+1)-s_j(2t+1+\tau)} \\ &= \begin{cases} \displaystyle\sum_{t=0}^{2^n-2} \omega^{s_i(2t)-s_j(2(t+\tau_1))} + \sum_{t=0}^{2^n-2} \omega^{s_i(2t+1)-s_j(2(t+\tau_1)+1)} & \text{if } \tau = 2\tau_1 \\ \displaystyle\sum_{t=0}^{2^n-2} \omega^{s_i(2t)-s_j(2(t+\tau_1)+1)} + \sum_{t=0}^{2^n-2} \omega^{s_i(2t+1)-s_j(2(t+\tau_1)+2)} & \text{if } \tau = 2\tau_1 + 1 \end{cases} \\ &= \begin{cases} \displaystyle\sum_{t=0}^{2^n-2} \omega^{s_i(2t)-s_{j-(2^e-1)}(2(t+\tau_1))-2} \\ \quad + \displaystyle\sum_{t=0}^{2^n-2} \omega^{s_i(2t+1)-s_{j-(2^e-1)}(2(t+\tau_1)+1)} & \text{if } \tau = 2\tau_1 \\ \displaystyle\sum_{t=0}^{2^n-2} \omega^{s_i(2t)-s_{j-(2^e-1)}(2(t+\tau_1)+1)} \\ \quad + \displaystyle\sum_{t=0}^{2^n-2} \omega^{s_i(2t+1)-s_{j-(2^e-1)}(2(t+\tau_1)+2)-2} & \text{if } \tau = 2\tau_1 + 1 \end{cases} \\ &= \begin{cases} R_{j,i}(\tau) & \text{if } \tau = 2\tau_1 \\ -R_{j,i}(\tau) & \text{if } \tau = 2\tau_1 + 1. \end{cases} \end{aligned}$$

We complete the proof using the results obtained in the proof of Theorem 2.3.3. ■

2.3.3 Constructions of Optimal Quaternary LCZ sequence sets

In this section we define a larger set $\mathcal{S}$ as a union of the sets $\mathcal{S}_1$ and $\mathcal{S}_2$ and prove that the set $\mathcal{S}$ is an optimal LCZ sequence set.

Definition 2.3.8 *Let $\mathcal{S}$ be the sequence set of $2(2^e-1)$ sequences of period $2(2^n-1)$ defined as*

$$\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2. \tag{2.37}$$

We immediately have the following theorem.

Theorem 2.3.9 *The set $\mathcal{S}$ is a quaternary LCZ sequence set with parameters*

$$\left(2(2^n-1), 2(2^e-1), \frac{2^n-1}{2^e-1}, 2\right).$$

Proof. We complete the proof using Theorem 2.3.6, Theorem 2.3.7 and the Definition 2.1.2 of LCZ sequence set. ■

Similar to the orthogonal transformation (2.3) described in Section 2.1, we can transform the LCZ set $\mathcal{S}$ (2.37) to the set $\mathcal{S}'$ defined as

$$\mathcal{S}' = \{s_i(t) | 0 \le t \le 2(2^n-1)-1,\ 1 \le i \le 2^{e+1}-3\},$$

where

$$s_0(t) = \begin{cases} 2\mathrm{tr}\left(\alpha^{t_1}\right) + 1, & t = 2t_1 \\ 2\mathrm{tr}\left(\alpha^{t_1+2^{n-1}}\right), & t = 2t_1+1, \end{cases}$$

$$s_{2^e-1}(t) = \begin{cases} 2\mathrm{tr}\left(\alpha^{t_1}\right) + 3, & t = 2t_1 \\ 2\mathrm{tr}\left(\alpha^{t_1+2^{n-1}}\right), & t = 2t_1+1, \end{cases}$$

and for $1 \le i \le 2^{e+1}-3$ with $i \ne 2^e-1$

$$s_i(t) = \begin{cases} \mathrm{tr}\left(\alpha^{t_1}\right) + 2\mathrm{tr}\left(\alpha^{t_1}\theta^i\right) + c_i, & t = 2t_1 \\ 3\mathrm{tr}\left(\alpha^{t_1+2^{n-1}}\right) + 2\mathrm{tr}\left(\alpha^{t_1+2^{n-1}}\theta^i\right), & t = 2t_1+1. \end{cases}$$

provided that $c_i = 1$ for $1 \le i \le 2^e - 2$ and $c_i = 3$ for $2^e \le i \le 2^{e+1} - 3$.

We immediately have the following result. We give the result without the proof since the proof directly follows from the same steps as in the proof of Theorem 2.3.9.

Proposition 2.3.10 *The set $\mathcal{S}'$ is a quaternary LCZ sequence set with parameters*

$$\left(2(2^n - 1), 2(2^e - 1), \frac{2^n - 1}{2^e - 1}, 2\right).$$

These new families are optimal with respect to Tang, Fan and Matsufuji bound (2.1). The optimality is shown in the following corollary.

Corollary 2.3.11 *Let n, e be positive integers such that $n \ge 3$, $e|n$ and $e \ne n$. Let $\mathcal{S}$ be a quaternary LCZ sequence set with parameters $\left(2(2^n - 1), 2(2^e - 1), \frac{2^n - 1}{2^e - 1}, 2\right)$. Then the set $\mathcal{S}$ is optimal with respect to Tang, Fan and Matsufuji bound (2.1).*

Proof. Here we show that if e, n satisfies the above conditions, larger set satisfying (2.1) cannot exist for a given $(N, L, \epsilon) = \left(2(2^n - 1), \frac{2^n - 1}{2^e - 1}, 2\right)$.

Let $\mathcal{S}$ be a queternary LCZ sequence set with parameters (N, M, L, ϵ). Then, clearly we have

$$ML - 1 = 2(2^e - 1)\frac{2^n - 1}{2^e - 1} - 1 = 2^{n+1} - 3,$$

$$\frac{N(N-1)}{N - \epsilon^2} = \frac{2(2^n - 1)(2(2^n - 1) - 1)}{2(2^n - 1) - 2^2} = 2^{n+1} - 3 + \frac{2^{n+3} - 12}{2^{n+1} - 6},$$

and

$$(M + 1)L - 1 = \left(2(2^e - 1) + 1\right)\frac{2^n - 1}{2^e - 1} - 1 = 2^{n+1} - 3 + \frac{2^n - 1}{2^e - 1}.$$

Clearly, $\frac{2^{n+3} - 12}{2^{n+1} - 6} < \frac{2^n - 1}{2^e - 1}$ for $n \ge 3$, $e|n$ and $e \ne n$, which completes the proof. ■

We give an example of family $\mathcal{S}$ and an example of family $\mathcal{S}'$ for some specific parameters.

Example 2.3.12 *Let $n = 4$, $e = 2$ and α be a primitive element in $\mathbb{F}_{2^4}$, that is, the root of $x^4 + x + 1 \in \mathbb{F}_2[x]$ and θ be a primitive element in $\mathbb{F}_{2^2}$. Then $\mathcal{S}$ is an optimal quaternary LCZ sequence set with parameters $(30, 6, 5, 2)$ defined as*

$$\mathcal{S} = \{s_i(t) | 0 \le i \le 5,\ 0 \le t \le 29\}$$

where

$$\begin{aligned}
s_0(t) &= [00020022020222200020022020222 2], \\
s_1(t) &= [02212013230133302232031210311 1], \\
s_2(t) &= [02232031210311102212013230133 3], \\
s_3(t) &= [20222002222202002000220000020 2], \\
s_4(t) &= [22010033032113100212233230113 1], \\
s_5(t) &= [22030011012331300232211210331 3].
\end{aligned}$$

Remark 2.3.13 *The LCZ sequence set in Example 2.3.12 has correlation values in the set*

$$\{0, \pm 2, \pm 14, \pm 30, \pm 16\omega\}.$$

The above correlation values show that the obtained (30,6,5,2) LCZ sequence set in Example 2.3.12 is different from the LCZ sequence sets in Example 2.2.4 and Example 2.2.5, since they have some different correlation values.

Example 2.3.14 *By transforming the LCZ set $\mathcal{S}$ in Example 2.3.14 to the set $\mathcal{S}'$, we obtain the following optimal quaternary LCZ sequence set with parameters* $(30, 6, 5, 2)$

$$\mathcal{S}' = \{s_i(t) | 0 \le i \le 5,\ 0 \le t \le 29\}$$

where

$$\begin{aligned}
s_0(t) &= [10121032121232301030123030323 2], \\
s_1(t) &= [12313023331103003202132220012 1], \\
s_2(t) &= [12333001311321203222110200230 3], \\
s_3(t) &= [30323012323212103010321010121 2], \\
s_4(t) &= [32111003133123201222330200210 1], \\
s_5(t) &= [32131021113301001202312220032 3].
\end{aligned}$$

Remark 2.3.15 *The LCZ sequence set in Example 2.3.14 has correlation values in the set*

$$\{0, -2, 14, \pm 16, 30, 2\omega, -14\omega, \pm 16\omega, -30\omega\}.$$

The above correlation values show that the obtained (30,6,5,2) LCZ sequence set in Example 2.3.14 is different from the LCZ sequence sets in Example 2.2.4, Example 2.2.5 and Example 2.3.12, since they have some different correlation values.

CHAPTER 3

HIGHLY DEGENERATE QUADRATIC FORMS OVER $\mathbb{F}_{2^k}$

Let $q = 2^t$ for some positive integer t. For positive integer k let $\mathbb{F}_q$ and $\mathbb{F}_{q^k}$ denote the finite fields with q and q^k elements. Let $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ denote the trace map from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$. We denote $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ by Tr throughout this chapter.

Let $R(x) = \epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_h x^{q^h} \in \mathbb{F}_{q^k}[x]$ be an $\mathbb{F}_q$-linearized polynomial, with h is a positive integer and $\epsilon_h \neq 0$. We consider the quadratic forms of the form

$$Q_R(x) = \mathrm{Tr}\left(xR(x)\right).$$

These quadratic forms have many applications in coding theory, cryptography and related areas [28, 35, 43]. For example, they are used to construct authentication codes [5, 29, 30], to construct certain sequences [19, 23, 24], to construct curves with many rational points [3, 6, 7, 9]. In these applications one has to find the number of solutions of the equation $Q_R(x) = 0$ in $\mathbb{F}_{q^k}$.

Let $N(k)$ denote the cardinality

$$N(k) = \left|\left\{x \in \mathbb{F}_{q^k} \mid Q_R(x) = 0\right\}\right|.$$

In this chapter we determine $N(k)$ exactly if the coefficients of $R(x)$ are in $\mathbb{F}_4$ and corresponding quadratic form $Q_R(x)$ has codimension 2 radical. We apply these results to obtain maximal and minimal Artin-Schreier curves.

Here we note that $N(k)$ is known up to certain parameters. From [26, Theorem 6.30, Theorem 6.32] it is known that

$$N(k) = q^{k-1} + \Lambda(Q_R)(q-1)q^{\frac{k+w}{2}-1},$$

where w is dimension of the associated radical and $\Lambda(Q_R)$ is the invariant (or discriminant) of the associated quadratic form Q_R with $\Lambda(Q_R) \in \{0, 1, -1\}$.

There are some attempts to determine $\Lambda(Q_R)$ and w explicitly for some special choices of $R(x)$. For the case k is even, in [3] the authors considered smooth, geometrically irreducible projective curves over $\mathbb{F}_{q^k}$ which are given by the plane equations of the form

$$y^q - y = xR(x). \tag{3.1}$$

Using suitable bilinear forms the number of $\mathbb{F}_{q^k}$-rational points of the curves in the form (3.1) up to certain invariants including the radical and the discriminant of the corresponding bilinear form is determined in [3, Theorem 3.1]. However it seems difficult to determine these invariants and hence the number of $\mathbb{F}_{q^k}$-rational points of the curves in the form (3.1) exactly and explicitly in general. A general result for the case $R(x) = \epsilon x^{q^h}$, only a single term, is given in [23, 31]. Furthermore, in [6] the author determines $\Lambda(Q_R)$ and w explicitly for all $R(x)$ having coefficients in $\mathbb{F}_2$. We extend the results in [6] by using similar techniques.

3.1 Preliminaries

In this section we recall some preliminaries and give some useful results which will be used in this chapter.

Let $R(x) = \epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_h x^{q^h} \in \mathbb{F}_{q^k}[x]$ be an $\mathbb{F}_q$-linearized polynomial with $h \geq 0$ and $\epsilon_h \neq 0$.

Let B_R be the symmetric bilinear form on the $\mathbb{F}_q$-linear vector space $\mathbb{F}_{q^k}$ defined as

$$\begin{aligned} B_R : \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} &\to \mathbb{F}_q \\ (x, y) &\mapsto \mathrm{Tr}\left(xR(y) + yR(x)\right). \end{aligned}$$

Let Q_R be the quadratic form defined as

$$\begin{aligned} Q_R : \mathbb{F}_{q^k} &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}\left(xR(x)\right). \end{aligned}$$

Let W_R be the radical of B_R,

$$W_R = \{x \in \mathbb{F}_{q^k} : B_R(x, y) = 0 \quad \text{for each } y \in \mathbb{F}_{q^k}\}.$$

Let w be the $\mathbb{F}_q$-dimension

$$w = \dim_{\mathbb{F}_q} W_R$$

of W_R. It is known that the codimension of the radical, $k - w$ is always even [6].

Now we have the following useful results from [6].

Proposition 3.1.1 ([6]) *Let Q_R be a quadratic form from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$. Let $w = \dim_{\mathbb{F}_q} W_R$ and $h = \frac{k-w}{2}$. Then there exist $c, a_1, b_1, \ldots, a_h, b_h \in \mathbb{F}_{q^k}$, independent over $\mathbb{F}_q$, such that*

$$Q_R(x) = \begin{cases} \mathrm{Tr}(cx)^2 + \sum_{i=1}^{h} \mathrm{Tr}(a_i x)\mathrm{Tr}(b_i x) & \text{if } \Lambda(Q_R) = 0, \\ \sum_{i=1}^{h} \mathrm{Tr}(a_i x)\mathrm{Tr}(b_i x) & \text{if } \Lambda(Q_R) = 1, \\ \mathrm{Tr}(a_1 x) + \mathrm{Tr}(b_2 x) + \sum_{i=1}^{h} \mathrm{Tr}(a_i x)\mathrm{Tr}(b_i x) & \text{if } \Lambda(Q_R) = -1. \end{cases}$$

Theorem 3.1.2 ([6]) *Let Q be a quadratic form from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$ and let $m = \lfloor k/2 \rfloor$. Then there exist unique $\epsilon_i \in \mathbb{F}_{q^k}$, $0 \le i \le m$, such that*

$$Q(x) = \mathrm{Tr}\left(x \sum_{i=0}^{m} \epsilon_i x^{q^i} \right),$$

except when k is even in which case ϵ_m is only unique modulo $\mathbb{F}_{q^m}$.

Throughout the remainder of this chapter we assume that $k = 2m$ for some positive integer m, $q = 2^t$ for some even integer t and

$$R(x) = \epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_{m-1} x^{q^{m-1}} \in \mathbb{F}_{q^k}[x]$$

be an $\mathbb{F}_q$-linearized polynomial, with $\epsilon_i \in \mathbb{F}_4$, $0 \le i \le m-1$. We consider the quadratic forms of the form

$$Q_R(x) = \mathrm{Tr}\left(xR(x)\right).$$

Using Proposition 3.1.1 and Theorem 3.1.2 we have the following important result. Note that the following result is an extension of the result in [6, Corollary 1.3], the coefficients ϵ_i's are taken from $\mathbb{F}_4$ instead of $\mathbb{F}_2$ which is the case in [6, Corollary 1.3].

Corollary 3.1.3 *Let* $R(x) = \sum_{i=0}^{m-1} \epsilon_i x^{q^i}$, *where each* $\epsilon_i \in \mathbb{F}_4$ *and* $k = 2m$ *for some positive integer m. Then* Q_R *has radical of dimension* $k-2$ *(codimension 2) if and only if there exist independent* $a, b, c \in \mathbb{F}_{q^k}$ *such that*

$$\epsilon_i = a^{q^i} b + a b^{q^i} \text{ for } 1 \leq i \leq m-1, \tag{3.2}$$

$$\epsilon_0 = \begin{cases} c^2 + ab & \text{if } \Lambda(Q_R) = 0 \\ ab & \text{if } \Lambda(Q_R) = 1 \\ a^2 + ab + sb^2 & \text{if } \Lambda(Q_R) = -1 \end{cases} \tag{3.3}$$

and

$$a^{q^m} b \in \mathbb{F}_{q^m}. \tag{3.4}$$

Here $s \in \mathbb{F}_q$ *is an element with* $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = s + s^2 + \cdots + s^{q/2} = 1$.

Proof. The same proof of [6, Corollary 1.3] works if we take the coefficients ϵ_i's from $\mathbb{F}_4$ instead of $\mathbb{F}_2$. ■

3.1.1 Some Useful Results

In this section we present some technical lemmas which are useful in the proof of Theorem 3.2.1.

Lemma 3.1.4 *[6] Let* $u = x + y$ *and* $v = xy$. *Then*

$$x^{2^n+1} + y^{2^n+1} = u^{2^n+1} + \sum_{i=0}^{n-1} u^{2^n+1-2^{i+1}} v^{2^i}.$$

Lemma 3.1.5 *Let* $q = 2^t$ *for some even integer t. Then there exist* $a, b \in \mathbb{F}_{q^2}$ *linearly independent over* $\mathbb{F}_q$ *such that*

$$\begin{aligned} a^2 + ab + sb^2 &= 0 \\ a^q b + a b^q &= e, \end{aligned}$$

where $s \in \mathbb{F}_q$ *is an element with* $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ *and* $e \in \mathbb{F}_4 \backslash \{0\}$.

Proof. Fix $s \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ and let $d \in \mathbb{F}_4 \backslash \{0\}$. Let $\alpha \in \mathbb{F}_{q^2}$ be a root of $x^2 + x + s$ and $\beta \in \mathbb{F}_{q^2}$ be a primitive element. Now we have

$$\alpha^2 + \alpha + s = 0. \tag{3.5}$$

Taking continuous squares of (3.5) gives

$$\begin{cases} \alpha^4 + \alpha^2 + s^2 &= 0, \\ \alpha^8 + \alpha^4 + s^4 &= 0, \\ & \vdots \\ \alpha^q + \alpha^{q/2} + s^{q/2} &= 0. \end{cases} \tag{3.6}$$

Adding each equations in (3.5) and (3.6) we have

$$\alpha^q + \alpha + s + s^2 + \cdots + s^{q/2} = 0,$$

which implies

$$\alpha^q + \alpha + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 0,$$

that is,

$$\alpha^q + \alpha = 1. \tag{3.7}$$

Therefore $\alpha \notin \mathbb{F}_q$ and $x^2 + x + s$ is irreducible over $\mathbb{F}_q$.

Set $b = d\beta^{q-1}$ and $a = \alpha b$. As $\dfrac{a}{b} = \alpha \notin \mathbb{F}_q$, a and b are linearly independent over $\mathbb{F}_q$. Now,

$$\begin{aligned} a^2 + ab + sb^2 &= b^2\left(\frac{a^2}{b^2} + \frac{a}{b} + s\right) \\ &= b^2(\alpha^2 + \alpha + s) \\ &= 0, \end{aligned}$$

and using (3.7)

$$\begin{aligned} a^q b + ab^q &= b^{q+1}((a/b)^q + a/b) \\ &= (d\beta^{q-1})^{q+1}\left(\alpha^q + \alpha\right) \\ &= d^{q+1}\beta^{q^2-1}\left(\alpha^q + \alpha\right) \\ &= d^2, \end{aligned}$$

as $d \in \mathbb{F}_4$. Hence, we obtain the desired result. ■

Lemma 3.1.6 *Let $q = 2^t$ for some even integer t. Then there exist $a, b \in \mathbb{F}_{q^2}$ linearly independent over $\mathbb{F}_q$ such that*

$$\begin{aligned} a^2 + ab + sb^2 &= d \\ a^q b + ab^q &= d, \end{aligned}$$

where $s \in \mathbb{F}_q$ is an element with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ and $d \in \mathbb{F}_4 \backslash \{0\}$.

Proof. Fix $s \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$. Then $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s+1) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ as $q = 2^t$ for some even integer t. Thus $x^2 + x + s + 1$ is irreducible over $\mathbb{F}_q$ by the same reasoning as in the proof of Lemma 3.1.5. Let $\beta \in \mathbb{F}_{q^2}$ be a root of $x^2 + x + s + 1$, that is,

$$\beta^2 + \beta + s + 1 = 0, \tag{3.8}$$

and therefore

$$\beta^q + \beta = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s+1) = 1. \tag{3.9}$$

Set $a_i = d^i\beta$ and $b_i = d^i$, where $i \in \{1, 2, 3\}$ and $d \in \mathbb{F}_4 \backslash \{0\}$. As $\dfrac{a_i}{b_i} = \beta \notin \mathbb{F}_q$, a_i and b_i are linearly independent over $\mathbb{F}_q$. Now using (3.8)

$$\begin{aligned} {a_i}^2 + a_i b_i + s{b_i}^2 &= d^{2i}(\beta^2 + \beta + s) \\ &= d^{2i} \end{aligned}$$

and using (3.9)

$$\begin{aligned} {a_i}^q b_i + a_i {b_i}^q &= \left(d^i\right)^{q+1} (\beta^q + \beta) \\ &= d^{2i}, \end{aligned}$$

as $d \in \mathbb{F}_4$. Hence, we obtain the desired results. ■

Lemma 3.1.7 *Let $q = 4^r$ for some odd integer r. Then there exist $a, b \in \mathbb{F}_{q^2}$ linearly independent over $\mathbb{F}_q$ such that*

$$\begin{aligned} ab &= d \\ a^q b + ab^q &= de, \end{aligned}$$

where $d \in \mathbb{F}_4 \backslash \{0\}$ and $e \in \mathbb{F}_4 \backslash \{0, 1\}$.

Proof. Let $\beta \in \mathbb{F}_{q^2}$ be primitive. Set $a_i = \beta^{i\frac{q^2-1}{5}}$ and $b_i = d\beta^{(5-i)\frac{q^2-1}{5}} = da_i^{-1}$, where $i \in \{1, 2\}$. As $\dfrac{b_i}{a_i} = da_i^{-2} \notin \mathbb{F}_q$, a_i and b_i are linearly independent over $\mathbb{F}_q$. Now,

$$\begin{aligned} a_i b_i &= a_i d a_i^{-1} = d \\ a^q b + a b^q &= a_i b_i (a_i^{q-1} + b_i^{q-1}) = de', \end{aligned}$$

where

$$\begin{aligned} (e')^4 &= \left(a_i^{q-1} + b_i^{q-1}\right)^4 \\ &= \left(\beta^{4i\frac{q^2-1}{5}}\right)^{q-1} + \left(d^{4(q-1)}\right)\left(\beta^{4(5-i)\frac{q^2-1}{5}}\right)^{q-1} \\ &= \left(\beta^{(5-i)\frac{q^2-1}{5}}\right)^{q-1} + \left(\beta^{i\frac{q^2-1}{5}}\right)^{q-1} \\ &= \left(d\beta^{(5-i)\frac{q^2-1}{5}}\right)^{q-1} + \left(\beta^{i\frac{q^2-1}{5}}\right)^{q-1} \\ &= e'. \end{aligned}$$

since $q = 4^r$ we have $3|q-1$, that is, $d^{q-1} = 1$. Also, we have $e' \neq 1$. If $e' = 1$, then we have $1 = x + x^{-1}$ where $x = a_i^{q-1}$. So $x^2 + x + 1 = 0$, which is not possible since a_i and b_i are linearly independent over $\mathbb{F}_q$. So by choosing $i = 1$ and $i = 2$, we obtain the desired results. ■

Lemma 3.1.8 *Let $q = 4^r$ for some even integer r. Then there exist $a, b \in \mathbb{F}_{q^2}$ linearly independent over $\mathbb{F}_q$ such that*

$$\begin{aligned} a^2 + ab + sb^2 &= de \\ a^q b + a b^q &= d, \end{aligned}$$

where $s \in \mathbb{F}_q$ is an element with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ and $d \in \mathbb{F}_4 \backslash \{0\}$ and $e \in \mathbb{F}_4 \backslash \{0, 1\}$.

Proof. Fix $s \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ and let $e \in \mathbb{F}_4 \backslash \{0, 1\}$. Then $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s+e) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ as r is even. Thus $x^2 + x + s + e$ is irreducible over $\mathbb{F}_q$ by the same reasoning as in the proof of Lemma 3.1.5. Let $\beta \in \mathbb{F}_{q^2}$ be a root $x^2 + x + s + e$,

$$\beta^2 + \beta + s + e = 0, \tag{3.10}$$

and therefore

$$\beta^q + \beta = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s + e) = 1. \tag{3.11}$$

Set $a_i = d^i\beta$ and $b_i = d^i$, where $i \in \{1, 2\}$ and $d \in \mathbb{F}_4\backslash\{0\}$. As $\dfrac{a_i}{b_i} = \beta \notin \mathbb{F}_q$, a_i and b_i are linearly independent over $\mathbb{F}_q$. Now using (3.10) and (3.11) we have

$$\begin{aligned} {a_i}^2 + a_i b_i + s{b_i}^2 &= d^{2i}(\beta^2 + \beta + s) = ed^{2i} \\ {a_i}^q b_i + a_i {b_i}^q &= d^{2i}(\beta^q + \beta) = d^{2i}. \end{aligned}$$

Therefore by choosing $i = 1$ and $i = 2$, we obtain the desired results. ■

Lemma 3.1.9 *[6] Let $v = 2^{3^r}$ and let*

$$g_v(x) = x^{v+1}\left(1 + x^{-2} + x^{-4} + \cdots + x^{-v}\right) + 1. \tag{3.12}$$

Let y be a root of $g_v(x)$ in some extension of $\mathbb{F}_q$. Then

1. $y \in \mathbb{F}_{v^3}\backslash\mathbb{F}_v$,
2. $y^{2v} + y^{v+1} + y^2 = 1$,
3. $y^{v^2+1} + y^{2v} = 1$,
4. $y^{v^2+v} + y^2 = 1$.

Lemma 3.1.10 *Let $q = 2^t$ for some even integer t and $3|k$. Then there exist $a, b, c \in \mathbb{F}_{q^3}$ linearly independent over $\mathbb{F}_q$ such that*

$$\begin{aligned} c^2 + ab &= d \\ a^q b + ab^q &= e \\ a^{q^2} b + ab^{q^2} &= e \\ a^{q^3} b + ab^{q^3} &= 0, \end{aligned}$$

where $d \in \mathbb{F}_4$, $e \in \mathbb{F}_4\backslash\{0\}$ and $d \neq e$.

Proof. This proof is similar to a part of the proof of [6, Theorem 2.4]. The differences are the appropriate choices of a, b and c.

Let $t = 3^r t_0$ for some positive integers r and t_0 with $\gcd(3, t_0) = 1$. Set $v = 2^{3^r}$ so that $q = 2^t = v^{t_0}$. Let y be a root of the polynomial g_v defined in (3.12). Then by Lemma 3.1.9 (part 1.) $y \in \mathbb{F}_{v^3} \subseteq \mathbb{F}_{q^3} \subseteq \mathbb{F}_{q^k}$.

Set $a = \alpha_1 y^v$, $b = \alpha_1 y$ and $c = \alpha_1(y^v + y) + \alpha_2$ for some $\alpha_1, \alpha_2 \in \mathbb{F}_4 \backslash \{0\}$.

Now, we first show that a, b, c are linearly independent over $\mathbb{F}_q$. If not then α_2 is in the $\mathbb{F}_q$-span of a and b, that is, 1 is in the $\mathbb{F}_q$-span of a and b. Hence $a = gb + h$ for some $g, h \in \mathbb{F}_q$, that is, $\alpha_1 y^v = g(\alpha_1 y) + h$. Then using Lemma 3.1.9 (part 2.) we obtain

$$\begin{aligned} 1 &= y^{2v} + y^{v+1} + y^2 \\ &= \alpha_1^{-2}(\alpha_1 g y + h)^2 + (\alpha_1 g y + h)y + y^2 \\ &= (g^2 + \alpha_1 g + 1)y^2 + hy + (\alpha_1^{-2} h^2). \end{aligned} \tag{3.13}$$

Now, $y \notin \mathbb{F}_v$ by Lemma 3.1.9 (part 1.), and so has degree 3 over $\mathbb{F}_v$. As $\gcd(3, t_0) = 1$, y has degree 3 over $\mathbb{F}_q = \mathbb{F}_{v^{t_0}}$ as well. Thus $1, y, y^2$ are independent over $\mathbb{F}_q$. Then (3.13) gives $h = 0$, and $\alpha_1^{-2} h^2 = 1$, that is, $h = \alpha_1 \in \mathbb{F}_4 \backslash \{0\}$, a contradiction. Thus a, b, c are independent over $\mathbb{F}_q$.

Now, we compute

$$\begin{aligned} c^2 + ab &= (\alpha_1(y^v + y) + \alpha_2)^2 + \alpha_1^2 y^{v+1} \\ &= \alpha_1^2 + \alpha_2 \text{ by Lemma 3.1.9 (part 2.).} \end{aligned}$$

Similarly, for the other equations we use again Lemma 3.1.9 and the following observation

$$y^q = y^{v^{t_0}} = \begin{cases} y^v \text{ if } t_0 \equiv 1 \mod 3, \\ y^{v^2} \text{ if } t_0 \equiv 2 \mod 3, \end{cases}$$

since $y \in \mathbb{F}_{v^3} \backslash \mathbb{F}_v$ by Lemma 3.1.9 (part 1.). Therefore,

$$\begin{aligned} a^q b + ab^q &= \alpha_1^2 \\ a^{q^2} b + ab^{q^2} &= \alpha_1^2 \\ a^{q^3} b + ab^{q^3} &= 0. \end{aligned}$$

Hence, we obtain the desired results. ■

Lemma 3.1.11 *Let $q = 2^t$ for some even integer t and $3|k$. Then there exist $a, b, c \in \mathbb{F}_{q^3}$ linearly independent over $\mathbb{F}_q$ such that*

$$\begin{aligned} ab &= d \\ a^q b + ab^q &= d \\ a^{q^2} b + ab^{q^2} &= d \\ a^{q^3} b + ab^{q^3} &= 0, \end{aligned}$$

where $d \in \mathbb{F}_4 \backslash \{0\}$.

Proof. This proof is similar to a part of the proof of [6, Theorem 2.4]. The differences are the appropriate choices of a, b and c.

Let γ be a primitive element of $\mathbb{F}_{q^3}$. As t is even, $q = 2^t \equiv 1 \mod 3$, and so $3|q^2+q+1$. Now, set $\varphi = \gamma^{(q^2+q+1)/3}$. Then φ has order $3(q-1)$ so that

$$\varphi^{2(q-1)} + \varphi^{q-1} + 1 = 0. \tag{3.14}$$

Set $a = \alpha\varphi^{-2}$ and $b = \alpha\varphi^2$ for some $\alpha \in \mathbb{F}_4 \backslash \{0\}$. Then a, b are linearly independent over $\mathbb{F}_q$ as $\frac{b}{a} = \varphi^4$ and $\varphi^{4(q-1)} \neq 1$, so that $\frac{b}{a} \notin \mathbb{F}_q$. Then, using (3.14) and $\varphi^{-2(q-1)} = \varphi^{(q-1)}$ we get

$$\begin{aligned} ab &= \alpha^2 \\ a^q b + ab^q &= \alpha^{q+1}\varphi^{-2(q-1)} + \alpha^{q+1}\varphi^{2(q-1)} = \alpha^2 \\ a^{q^2} b + ab^{q^2} &= \alpha^{q^2+1}\varphi^{-2(q^2-1)} + \alpha^{q^2+1}\varphi^{2(q^2-1)} = \alpha^2 \\ a^{q^3} b + ab^{q^3} &= 0. \end{aligned}$$

Hence, we obtain the desired results. ■

Lemma 3.1.12 *Let* $q = 4^r$ *for some even integer* r *and* $5|k$. *Then there exist* $a, b \in \mathbb{F}_{q^5}$ *linearly independent over* $\mathbb{F}_q$ *such that*

$$\begin{aligned} ab &= \alpha_0, \\ a^q b + ab^q &= \alpha_1, \\ a^{q^2} b + ab^{q^2} &= \alpha_2, \end{aligned}$$

where $\alpha_0, \alpha_1, \alpha_2 \in \mathbb{F}_4 \backslash \{0\}$ *and all are different.*

Proof. As $5|k$, we have $\mathbb{F}_{q^5} \subseteq K$ and since r is even we have $5|q^4+q^3+q^2+q+1$. Now, let $\mathbb{F}_{q^5}^* =< \gamma >$ and define $\beta = \gamma^{\frac{q^4+q^3+q^2+q+1}{5}}$. Then $order(\beta) = 5(q-1)$.

Now, set $\beta_1 = \beta^{3(q-1)} + \beta^{2(q-1)}$ and $\beta_2 = \beta^{q-1} + \beta^{4(q-1)}$. As $(\beta^{q-1})^5 = 1$, we obtain that $\beta_1 + \beta_2 = 1$. Also, we have $\beta_1^4 = \beta^{12(q-1)} + \beta^{8(q-1)} = \beta_1$ and similarly $\beta_2^4 = \beta_2$. Moreover, we know that $\beta_1 \neq \beta_2, \beta_1 \neq 1$ and $\beta_2 \neq 1$.

Set $a = e\beta$ and $b = e\beta^{-1}$ with $e \in \mathbb{F}_4 \backslash \{0\}$. They are independent over $\mathbb{F}_{q^5}$ as $(a/b)^{q-1} = \beta^{2(q-1)} \neq 1$.

Now, we compute

$$\begin{aligned} ab &= e^2, \\ a^q b + ab^q &= e^2(\beta^{q-1} + \beta^{1-q}) = e^2\beta_2, \\ a^{q^2} b + ab^{q^2} &= e^2((\beta^{q-1})^{q+1} + (\beta^{1-q})^{1+q}) = e^2(\beta^{2(q-1)} + \beta^{3(q-1)}) = e^2\beta_1, \end{aligned}$$

which completes the proof. ■

Lemma 3.1.13 *Let $v = 4^{5^r}$ and let*

$$f_v(x) = x^{v+1}\left(1 + ex^{-2} + e^2x^{-4} + ex^{-8} + e^2x^{-16} + \cdots + e^2x^{-v}\right) + d, \tag{3.15}$$

where $e, d \in \mathbb{F}_4\backslash\{0\}$ and $e \neq d$. Let y be a root of $f_v(x)$ in some extension of $\mathbb{F}_q$. Then

1. $y \in \mathbb{F}_{v^5}\backslash\mathbb{F}_v$,
2. $y^{2v} + de^2y^{v+1} + y^2 = d^2e^2$,
3. $y^{v^2+1} + y^{2v} = d^2e^2$,
4. $y^{v^3+1} + y^{v^2+v} = e$.

Proof. We have $f_v(y) = 0$, that is,

$$1 + ey^{-2} + e^2y^{-4} + ey^{-8} + \cdots + e^2y^{-v} = dy^{-(v+1)}. \tag{3.16}$$

Squaring (3.16) we get

$$1 + e^2y^{-4} + ey^{-8} + e^2y^{-16} + \cdots + ey^{-2v} = d^2y^{-2(v+1)}. \tag{3.17}$$

Now, adding (3.16) and (3.17), we obtain

$$ey^{-2} + ey^{-2v} = dy^{-(v+1)} + d^2y^{-2(v+1)}. \tag{3.18}$$

Then multiplying (3.18) by e^2y^{2v+2} we get (2).

Now take the square of (2) and multiply the result by y^{-4} to get

$$y^{4(v-1)} + d^2ey^{2(v-1)} + 1 = dey^{-4}. \tag{3.19}$$

Now, using (2) and (3.19) we get

$$y^{4(v-1)} = y^{v-1} + dy^{-2} + d^2e + dey^{-4} + 1. \tag{3.20}$$

Now, we can take the squares of (3.20) until to obtain $y^{v(v-1)}$ on the left hand side of the equation. At the end of this process we get

$$y^{v(v-1)} = y^{v-1} + de^2(ey^{-2} + e^2y^{-4} + \cdots + e^2y^{-v}) + d^2e + 1. \tag{3.21}$$

Now, using (3.16) and (3.21) we obtain

$$y^{v^2-v} + y^{v-1} = d^2e^2y^{-(v+1)}. \tag{3.22}$$

Note that, on the right hand side of the last equation we have the term $de^2 + d^2e + 1$ which is 0 in $\mathbb{F}_4$. Then multiplying (3.22) by y^{v+1} we get (3).

Now using (2) and (3) we have

$$y^{v^2+1} = de^2y^{v+1} + y^2, \tag{3.23}$$

and multiplying (3.23) by $y^{-(v+1)}$ we get

$$y^{v^2-v} = y^{-v+1} + de^2. \tag{3.24}$$

On the other hand, taking the v-th power of (3.22) and substituting y^{v^2-v} as in (3.22) we get

$$y^{v^3-v^2} + y^{v-1} = d^2e^2y^{-(v+1)} + d^2e^2y^{-(v^2+v)}. \tag{3.25}$$

Now multiplying (3.25) by y^{v^2+1} and using (3.24) we get (4).

Now using the above results we will show (1).

Taking the v-th power of (3.24) and multiplying the results by y^{v^2+v} we get

$$y^{v^3+v} + de^2y^{v^2+v} = y^{2v}. \tag{3.26}$$

Now multiplying (3.26) by y^{-v+1} and taking the v-th power of the result we get

$$y^{v^4+v} + de^2y^{v^3+v} = y^{v^2+v}. \tag{3.27}$$

Now combining (3.26) and (3.27) we get

$$y^{v^4+v} + (d^2e + 1)y^{v^2+v} = de^2y^{2v}. \tag{3.28}$$

Then multiplying (3.28) by y^{-v+1} and taking the v-th power of the result we get

$$y^{v^5+v} + (d^2e + 1)y^{v^3+v} = de^2y^{v^2+1}. \tag{3.29}$$

Again using (3.26) and multiplying the result by y^{-v} we get

$$y^{v^5} = (d^2e + 1)y^v + y^{v^2}. \tag{3.30}$$

Then using (3.23) and (3.30) we obtain that $y^{v^5} = y$, that is, $y \in \mathbb{F}_{v^5}$.

Lastly, if $y \in \mathbb{F}_v$, then we have $y^{v^2+1} + y^{2v} = (y^v)^v \cdot y + (y^v)^2 = y^2 + y^2 = 0$, which contradicts with (3). Thus $y \notin \mathbb{F}_v$. Therefore we obtain the desired results.

■

3.2 Main Results

In this section we first give our main result in Theorem 3.2.1. We determine $\Lambda(Q_R)$ and w explicitly for all $R(x)$ having coefficients in $\mathbb{F}_4$, which extend the results in [6]. In the proof of Theorem 3.2.1 we use the results obtained in Section 3.1.1 and we use similar arguments with the the proof of Theorem 2.4 in [6].

Define

$$A_j(\epsilon_1, \epsilon_2, \ldots, \epsilon_{j-1}; x) = \sum_{i=1, j\nmid i}^{m-1} \epsilon_{(i \mod j)} x^{q^i}.$$

Now we are ready to state our main result.

Theorem 3.2.1 *Let $R = \sum_{i=0}^{m-1} \epsilon_i x^{q^i}$, where each $\epsilon_i \in \mathbb{F}_4$ and $k = 2m$. Then Q_R has radical of dimension $k-2$ (codimension 2) if and only if*

1. *$4|k$ and $R = dx + A_2(\epsilon; x)$, where $d \in \mathbb{F}_4$ and $\epsilon \in \mathbb{F}_4\backslash\{0\}$ or*
2. *$3|k$ and $R = dx + A_3(\epsilon, \epsilon; x)$, where $d \in \mathbb{F}_4$ and $\epsilon \in \mathbb{F}_4\backslash\{0\}$ or*
3. *$5|k$ and $R = dx + A_5(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_1; x)$, where $d \in \mathbb{F}_4$ and $\epsilon_1, \epsilon_2 \in \mathbb{F}_4\backslash\{0\}$ with $\epsilon_1 \neq \epsilon_2$.*

The classification in these cases is given in Table 3.1.

Proof. In the first part of the proof we need to find all extensions $\mathbb{F}_{q^k}$, all independent $a, b, c \in \mathbb{F}_{q^k}$, and all ϵ_i, that satisfy (3.3) for $i = 0$, (3.2) for $1 \leq i \leq m-1$ and (3.4).

Table 3.1: Invariants of quadratic form $Q_R(x)$, where $R(x)$ has coefficients in $\mathbb{F}_4$.

k	q	R	$\Lambda(Q_R)$
$4\|k$	4^r, r odd	$dx + A_2(\epsilon; x)$, $d \neq 0$ and $d \neq \epsilon$	1
$4\|k$	4^r, r odd	$dx + A_2(\epsilon; x)$, $d = 0$ or $d = \epsilon$	-1
$4\|k$	4^r, r even	$dx + A_2(\epsilon; x)$	-1
$3\|k$	4^r	$dx + A_3(\epsilon, \epsilon; x)$, $d = \epsilon$	1
$3\|k$	4^r	$dx + A_3(\epsilon, \epsilon; x)$, $d \neq \epsilon$	0
$5\|k$	4^r, r even	$dx + A_3(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_1; x)$, $d \neq 0$, $d \neq \epsilon_1$, $d \neq \epsilon_2$	1
$5\|k$	4^r, r odd	$dx + A_3(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_1; x)$, $d \neq 0$, $d \neq \epsilon_1$, $d \neq \epsilon_2$	-1
$5\|k$	4^r	$dx + A_3(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_1; x)$, $d = 0$ or $d = \epsilon_1$ or $d = \epsilon_2$	0

For $1 \leq i \leq m-1$ we need the solutions of $\epsilon_i = a^{q^i} b + a b^{q^i}$. Set

$$u = a^{q-1} + b^{q-1} \text{ and } v = ab.$$

Then from (3.2) we have $uv = \epsilon_1$. Now, if $\epsilon_1 = 0$, then

$$0 = uv = \left(a^{q-1} + b^{q-1}\right) ab$$

which means either $a = 0$, $b = 0$ or $a^{q-1} = b^{q-1}$ (and so $\left(\frac{a}{b}\right)^{q-1} = 1$, that is, $a = \lambda b$ for some $\lambda \in \mathbb{F}_q$). This contradicts with the assumption that a and b are linearly independent over $\mathbb{F}_q$. Therefore $\epsilon_1 \neq 0$. So we have $u = \dfrac{\epsilon_1}{v}$.

Now using (3.2) we have

$$\begin{aligned} \epsilon_2 &= a^{q^2} b + a b^{q^2} \\ &= ab\left(\left(a^{q-1}\right)^{q+1} + \left(b^{q-1}\right)^{q+1}\right) \\ &= v\left[u^{q+1} + \sum_{i=0}^{t-1} u^{q+1-2^{i+1}} (v^{q-1})^{2^i}\right], \end{aligned} \tag{3.31}$$

by using Lemma 3.1.4. Then multiplying (3.31) by v^q, we obtain

$$v^q \epsilon_2 = \epsilon_1^{q+1} + \sum_{i=0}^{t-1} \epsilon_1^{q+1-2^{i+1}} \left(v^{q+1}\right)^{2^i}. \tag{3.32}$$

Then we must consider the following 3 cases.

Case 1. Assume that $\epsilon_1 \in \mathbb{F}_4 \backslash \{0\}$ and $\epsilon_2 = 0$.

Using (3.32) we have

$$\begin{aligned} 0 &= \epsilon_1^{q+1} + \sum_{i=0}^{t-1} \epsilon_1^{q+1-2^{i+1}} \left(v^{q+1}\right)^{2^i} \\ &= {\epsilon_1}^2 + v^{q+1} + \epsilon_1 \left(v^{q+1}\right)^2 + \left(v^{q+1}\right)^4 + \epsilon_1 \left(v^{q+1}\right)^8 + \cdots + \epsilon_1 \left(v^{q+1}\right)^{q/2}. \quad (3.33) \end{aligned}$$

Here we note that as $\epsilon_1 \in \mathbb{F}_4 \backslash \{0\}$ we have

$$\epsilon_1^{q+1} = \epsilon_1^q \epsilon_1 = \epsilon_1^2.$$

Now, squaring (3.33) gives

$$0 = \epsilon_1 + \left(v^{q+1}\right)^2 + \epsilon_1^2 \left(v^{q+1}\right)^4 + \left(v^{q+1}\right)^8 + \epsilon_1^2 \left(v^{q+1}\right)^{16} + \cdots + \epsilon_1^2 \left(v^{q+1}\right)^q. \quad (3.34)$$

Adding ϵ_1 times (3.34) to (3.33) we have

$$v^{q+1} + \left(v^{q+1}\right)^q = 0,$$

which implies that

$$v^{q^2-1} = 1.$$

So, we have $v = ab \in \mathbb{F}_{q^2}$. As $0 = \epsilon_2 = a^{q^2}b + ab^{q^2}$, we have $\left(\frac{a}{b}\right)^{q^2-1} = 1$, that is, $\frac{a}{b} \in \mathbb{F}_{q^2}$. Now using $ab, \frac{a}{b} \in \mathbb{F}_{q^2}$ we obtain that $a, b \in \mathbb{F}_{q^2}$. Now, since a and b are linearly independent over $\mathbb{F}_q$, we must have at least one of $a, b \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Say $a \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. So if $a \in \mathbb{F}_{q^k}$ then $2|k$.

Now, using (3.2) and $a, b \in \mathbb{F}_{q^2}$, we obtain that

$$\epsilon_{i+2} = \begin{cases} a^{q^i}b + ab^{q^i} = ab + ba = 0 & \text{if } i \text{ is even} \\ a^{q^i}b + ab^{q^i} = a^q b + ab^q = \epsilon_1 & \text{if } i \text{ is odd} \end{cases}$$

for $i \geq 1$. Therefore, $R = dx + A_2(\epsilon_1; x)$, where $d \in \mathbb{F}_4$ and $\epsilon_1 \in \mathbb{F}_4 \backslash \{0\}$.

Lastly, recall that $k = 2m$. So we have to check (3.4). If m is even then

$$a^{q^m}b = ab \in \mathbb{F}_{q^2} \subseteq \mathbb{F}_{q^m}.$$

On the other hand if m is odd then

$$a^{q^m}b = a^q b = a^{q-1}v = \frac{\epsilon_1 a^{q-1}}{u} \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q,$$

so that $a^{q^m}b \notin \mathbb{F}_{q^m}$. Hence, to have a solution in $\mathbb{F}_{q^k}$ we must have that m is even, that is, $4|k$.

Case 2. Assume that $\epsilon_1, \epsilon_2 \in \mathbb{F}_4 \backslash \{0\}$ and $\epsilon_2 = \epsilon_1$.

Using (3.32) we have

$$\epsilon_1 v^q = {\epsilon_1}^2 + v^{q+1} + \epsilon_1 \left(v^{q+1}\right)^2 + \left(v^{q+1}\right)^4 + \epsilon_1 \left(v^{q+1}\right)^8 + \cdots + \epsilon_1 \left(v^{q+1}\right)^{q/2}. \tag{3.35}$$

Squaring (3.35) gives

$$(\epsilon_1 v^q)^2 = \epsilon_1 + \left(v^{q+1}\right)^2 + \epsilon_1^2 \left(v^{q+1}\right)^4 + \left(v^{q+1}\right)^8 + \cdots + \epsilon_1^2 \left(v^{q+1}\right)^q. \tag{3.36}$$

Now adding ϵ_1 times (3.36) to (3.35) we have

$$\epsilon_1 v^q + v^{2q} = v^{q+1} + v^{q^2+q} \tag{3.37}$$

Now dividing each side of (3.37) by v^q we obtain

$$\epsilon_1 + v^q = v + v^{q^2} \tag{3.38}$$

Taking q-th power of (3.38) gives

$$\epsilon_1 + v^{q^2} = v^q + v^{q^3} \tag{3.39}$$

Adding (3.38) and (3.39) we have

$$v^{q^3} = v.$$

Moreover, (3.38) gives $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(v) = \epsilon_1$.

Now, set $y_0 = \epsilon_1^2 v a^{q-1}$ and $y_1 = \epsilon_1^2 v b^{q-1}$. Since

$$y_0 + y_1 = \epsilon_1^2 v \left(a^{q-1} + b^{q-1}\right) = \epsilon_1^2 v u = 1,$$

and $y_0 y_1 = \epsilon_1 v^{q+1}$, y_0 and y_1 are roots of

$$y^2 + y + \epsilon_1 v^{q+1} \in \mathbb{F}_{q^3}[y].$$

As

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_2}\left(\epsilon_1 v^{q+1}\right) &= \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i} + \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{q2^i} + \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{q^2 2^i} \\
&= \left(1 + \epsilon_1^2 v^q\right) + \left(1 + \epsilon_1^2 v^q\right)^q + \left(1 + \epsilon_1^2 v^q\right)^{q^2} \\
&= 1 + \epsilon_1^2 \mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(v) \\
&= 0.
\end{aligned}$$

Using [26, Corollary 3.79], we obtain that $y^2+y+\epsilon_1 v^{q+1}$ has its roots in $\mathbb{F}_{q^3}$. Therefore, a^{q-1} and b^{q-1} are in $\mathbb{F}_{q^3}$.

Now, using $y^2 = y + \epsilon_1 v^{q+1}$, we get

$$y^q = y + \epsilon_1 v^{q+1} + \left(\epsilon_1 v^{q+1}\right)^2 + \cdots + \left(\epsilon_1 v^{q+1}\right)^{q/2},$$

which immediately gives

$$y^q = y + \epsilon_1^2 v^q + 1 \tag{3.40}$$

and

$$y^{q^2} = y + \epsilon_1^2 v + 1. \tag{3.41}$$

Using, (3.40) and (3.41) we obtain that $y^{q^2+q+1} = v^{q^2+q+1}$, that is, $a^{q^3-1} = 1 = b^{q^3-1}$. Hence, $a, b \in \mathbb{F}_{q^3}$. Therefore, using (3.2) and $a, b \in \mathbb{F}_{q^3}$, we obtain that

$$\epsilon_3 = a^{q^3} b + a b^{q^3} = ab + ab = 0,$$

and

$$\epsilon_{i+3} = \begin{cases} a^{q^i} b + a b^{q^i} = ab + ba = 0 & \text{if } i \equiv 0 \bmod 3 \\ a^{q^i} b + a b^{q^i} = a^q b + a b^q = \epsilon_1 & \text{if } i \equiv 1 \bmod 3 \\ a^{q^i} b + a b^{q^i} = a^{q^2} b + a b^{q^2} = \epsilon_2 = \epsilon_1 & \text{if } i \equiv 2 \bmod 3 \end{cases}$$

for $i \geq 1$. Therefore, $R = dx + A_3(\epsilon_1, \epsilon_1; x)$, where $d \in \mathbb{F}_4$ and $\epsilon_1 \in \mathbb{F}_4 \backslash \{0\}$. Again, similar to the previous case, we must have at least one of $a, b \in \mathbb{F}_{q^3} \backslash \mathbb{F}_q$, since they are linearly independent over $\mathbb{F}_q$. Say $a \in \mathbb{F}_{q^3} \backslash \mathbb{F}_q$. So if $a \in \mathbb{F}_{q^k}$ then $3|k$. Moreover, as $k = 2m$ and $3|k$ we have $3|m$. Then (3.4) is satisfied since

$$a^{q^m} b \in \mathbb{F}_{q^3} \subseteq \mathbb{F}_{q^m}.$$

Case 3. Assume that $\epsilon_1, \epsilon_2 \in \mathbb{F}_4 \backslash \{0\}$ and $\epsilon_2 \neq \epsilon_1$.

Using (3.32) we have

$$\epsilon_2 v^q = {\epsilon_1}^2 + v^{q+1} + \epsilon_1 \left(v^{q+1}\right)^2 + \left(v^{q+1}\right)^4 + \epsilon_1 \left(v^{q+1}\right)^8 + \cdots + \epsilon_1 \left(v^{q+1}\right)^{q/2}. \tag{3.42}$$

Squaring (3.42) gives

$$(\epsilon_2 v^q)^2 = \epsilon_1 + \left(v^{q+1}\right)^2 + \epsilon_1^2 \left(v^{q+1}\right)^4 + \left(v^{q+1}\right)^8 + \cdots + \epsilon_1^2 \left(v^{q+1}\right)^q. \tag{3.43}$$

Now adding ϵ_1 times (3.43) to (3.42) we have

$$\epsilon_2 v^q + \epsilon_1 \epsilon_2^2 v^{2q} = v^{q+1} + v^{q^2+q} \tag{3.44}$$

Now dividing each side of (3.44) by v^q we obtain

$$\epsilon_2 + \epsilon_1 \epsilon_2^2 v^q = v + v^{q^2} \tag{3.45}$$

Taking q-th powers of (3.45) gives

$$v^{q^3} = \epsilon_2 + \epsilon_1 \epsilon_2^2 v^{q^2} + v^q \tag{3.46}$$

$$v^{q^4} = \epsilon_2 + \epsilon_1 \epsilon_2^2 v^{q^3} + v^{q^2} \tag{3.47}$$

$$v^{q^5} = \epsilon_2 + \epsilon_1 \epsilon_2^2 v^{q^4} + v^{q^3} \tag{3.48}$$

Now (3.45), (3.46), (3.47) and (3.48) gives

$$v^{q^5} = v.$$

Moreover, we have $\mathrm{Tr}_{\mathbb{F}_{q^5}/\mathbb{F}_q}(v) = \epsilon_1 + \epsilon_2$.

Similar to the previous case, set $y_0 = \epsilon_1^2 v a^{q-1}$ and $y_1 = \epsilon_1^2 v b^{q-1}$. Since $y_0 + y_1 = 1$ and $y_0 y_1 = \epsilon_1 v^{q+1}$, y_0 and y_1 are roots of

$$y^2 + y + \epsilon_1 v^{q+1} \in \mathbb{F}_{q^5}[y].$$

As

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{F}_{q^5}/\mathbb{F}_2}\left(\epsilon_1 v^{q+1}\right) &= \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i} + \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{q 2^i} + \cdots + \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{q^4 2^i} \\
&= (1 + \epsilon_1 \epsilon_2 v^q) + (1 + \epsilon_1 \epsilon_2 v^q)^q + \cdots + (1 + \epsilon_1 \epsilon_2 v^q)^{q^4} \\
&= 1 + \epsilon_1 \epsilon_2 \mathrm{Tr}_{\mathbb{F}_{q^5}/\mathbb{F}_q}(v) \\
&= 0.
\end{aligned}$$

Using [26, Corollary 3.79], we obtain that $y^2 + y + \epsilon_1 v^{q+1}$ has its roots in $\mathbb{F}_{q^5}$. Therefore, a^{q-1} and b^{q-1} are in $\mathbb{F}_{q^5}$.

Let $\mathrm{Norm}_{\mathbb{F}_{q^5}/\mathbb{F}_q}$ be the norm map from $\mathbb{F}_{q^5}$ onto $\mathbb{F}_q$ defined by

$$\begin{aligned}
\mathrm{Norm}_{\mathbb{F}_{q^5}/\mathbb{F}_q} : \mathbb{F}_{q^5} &\to \mathbb{F}_q \\
x &\mapsto x^{1+q+q^2+q^3+q^4}.
\end{aligned}$$

Now, taking q-th power of the equation $y^2 + y = e_1 v^{q+1}$, we obtain that

$$y^{q^i}(y+1)^{q^i} = \epsilon_1 v^{q^{i+1}+q^i}, \text{ for } i = 0, 1, \dots 4.$$

Then multiplying all of them, we get

$$\prod_{i=0}^{4} y^{q^i}(y+1)^{q^i} = \prod_{i=0}^{4} \epsilon_1 v^{q^{i+1}+q^i}$$

which implies that

$$\text{Norm}(y)\text{Norm}(y+1) = \left(\epsilon_1 v^{q^4+q^3+q^2+q+1}\right)^2.$$

On the other hand, y and $y+1$ are roots of $y^2 + y + e_1 v^{q+1} = 0$. Therefore, $\text{Norm}(y) = \text{Norm}(y+1)$ by [26, Equation 2.3]. Hence, we obtain that

$$\left(y^{q^4+q^3+q^2+q+1}\right)^2 = \left(\epsilon_1 v^{q^4+q^3+q^2+q+1}\right)^2,$$

which gives

$$y^{q^4+q^3+q^2+q+1} = \epsilon_1 v^{q^4+q^3+q^2+q+1}$$

and dividing by $\epsilon_1 v^{q^4+q^3+q^2+q+1}$, we get $a^{q^5-1} = 1 = b^{q^5-1}$.

Hence, $a, b \in \mathbb{F}_{q^5}$. So, as $\epsilon_1, \epsilon_2 \in \mathbb{F}_4$ we have

$$\begin{aligned}
\epsilon_1 = \epsilon_1^{q^4} &= (a^q b + ab^q)^{q^4} = \epsilon_4, \\
\epsilon_2 = \epsilon_2^{q^3} &= \left(a^{q^2} b + ab^{q^2}\right)^{q^3} = \epsilon_3, \\
\epsilon_5 &= a^{q^5} b + ab^{q^5} = ab + ab = 0,
\end{aligned}$$

and

$$\epsilon_{i+5} = \begin{cases}
a^{q^i} b + ab^{q^i} = ab + ba = 0 & \text{if } i \equiv 0 \bmod 5 \\
a^{q^i} b + ab^{q^i} = a^q b + ab^q = \epsilon_1 & \text{if } i \equiv 1 \bmod 5 \\
a^{q^i} b + ab^{q^i} = a^{q^2} b + ab^{q^2} = \epsilon_2 & \text{if } i \equiv 2 \bmod 5 \\
a^{q^i} b + ab^{q^i} = a^{q^3} b + ab^{q^3} = \epsilon_3 = \epsilon_2 & \text{if } i \equiv 3 \bmod 5 \\
a^{q^i} b + ab^{q^i} = a^{q^4} b + ab^{q^4} = \epsilon_4 = \epsilon_1 & \text{if } i \equiv 4 \bmod 5
\end{cases}$$

for $i \geq 1$. Therefore, $R = dx + A_5(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_1; x)$, where $d \in \mathbb{F}_4$ and $\epsilon_1, \epsilon_2 \in \mathbb{F}_4 \backslash \{0\}$ with $\epsilon_2 \neq \epsilon_1$. Again, similar to the previous case, we must have at least one of $a, b \in \mathbb{F}_{q^5} \backslash \mathbb{F}_q$, since they are linearly independent over $\mathbb{F}_q$. Say $a \in \mathbb{F}_{q^5} \backslash \mathbb{F}_q$. So if $a \in \mathbb{F}_{q^k}$ then $5|k$. Moreover, as $k = 2m$ and $5|k$ we have $5|m$. Then (3.4) is satisfied since

$$a^{q^m} b \in \mathbb{F}_{q^5} \subseteq \mathbb{F}_{q^m}.$$

The above three cases complete the first part of the proof.

For the second part of the proof again we must consider the following three cases.

Case 1. Assume that $4|k$ and $R = dx + A_2(\epsilon; x)$, where $d \in \mathbb{F}_4$ and $\epsilon \in \mathbb{F}_4 \backslash \{0\}$.

In this case we have the following four subcases depending on the invariant of R.

- Assume that $d = 0$.

  Using Lemma 3.1.5 we can find $a, b \in \mathbb{F}_{q^2}$ linearly independent over $\mathbb{F}_q$ and $s \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ such that

  $$\begin{aligned} a^2 + ab + sb^2 &= 0 \\ a^q b + ab^q &= \epsilon. \end{aligned}$$

  As $a, b \in \mathbb{F}_{q^2}$, we have

  $$\epsilon_{i+2} = \begin{cases} a^{q^i} b + ab^{q^i} = ab + ba = 0 & \text{if } i \text{ is even} \\ a^{q^i} b + ab^{q^i} = a^q b + ab^q = \epsilon & \text{if } i \text{ is odd} \end{cases}$$

  for $i \geq 1$. Moreover, as $4|k = 2m$, (3.4) is satisfied since $a^{q^m} b \in \mathbb{F}_{q^2} \subseteq \mathbb{F}_{q^m}$.

  Hence, $\mathrm{Tr}(ax)^2 + \mathrm{Tr}(ax)\mathrm{Tr}(bx) + s\mathrm{Tr}(bx)^2 = \mathrm{Tr}(xR(x))$ is a form of codimension 2 radical and invariant -1.

- Assume that $\epsilon = d$.

  Using Lemma 3.1.6 we can find $a, b \in \mathbb{F}_{q^2}$ linearly independent over $\mathbb{F}_q$ and $s \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ such that

  $$\begin{aligned} a^2 + ab + sb^2 &= d \\ a^q b + ab^q &= d. \end{aligned}$$

  As $a, b \in \mathbb{F}_{q^2}$, similar to the above case (3.2) and (3.4) is satisfied.

  Hence, $\mathrm{Tr}(ax)^2 + \mathrm{Tr}(ax)\mathrm{Tr}(bx) + s\mathrm{Tr}(bx)^2 = \mathrm{Tr}(xR(x))$ is a form of codimension 2 radical and invariant -1.

- Assume that $d \neq 0$, $\epsilon \neq d$ and let $q = 4^r$ for some even r.

  Using Lemma 3.1.8 we can find $a, b \in \mathbb{F}_{q^2}$ linearly independent over $\mathbb{F}_q$ and $s \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ such that

  $$\begin{aligned} a^2 + ab + sb^2 &= d \\ a^q b + ab^q &= \epsilon. \end{aligned}$$

As $a, b \in \mathbb{F}_{q^2}$, similar to the above cases (3.2) and (3.4) is satisfied.

Hence, $\mathrm{Tr}(ax)^2 + \mathrm{Tr}(ax)\mathrm{Tr}(bx) + s\mathrm{Tr}(bx)^2 = \mathrm{Tr}(xR(x))$ is a form of codimension 2 radical and invariant -1.

– Assume that $d \neq 0$, $\epsilon \neq d$ and let $q = 4^r$ for some odd r.

Using Lemma 3.1.7 we can find $a, b \in \mathbb{F}_{q^2}$ linearly independent over $\mathbb{F}_q$ such that

$$\begin{aligned} ab &= d \\ a^q b + ab^q &= \epsilon. \end{aligned}$$

As $a, b \in \mathbb{F}_{q^2}$, similar to the above cases (3.2) and (3.4) is satisfied.

Hence, $\mathrm{Tr}(ax)\mathrm{Tr}(bx) = \mathrm{Tr}(xR(x))$ is a form of codimension 2 radical and invariant 1.

Case 2. Assume that $3|k$ and $R = dx + A_3(\epsilon, \epsilon; x)$, where $d \in \mathbb{F}_4$ and $\epsilon \in \mathbb{F}_4 \backslash \{0\}$.

In this case we have the following three subcases depending on the invariant of R.

– Assume that $\epsilon \neq d$.

Using Lemma 3.1.10 we can find $a, b, c \in \mathbb{F}_{q^3}$ linearly independent over $\mathbb{F}_q$ such that

$$\begin{aligned} c^2 + ab &= d \\ a^q b + ab^q &= \epsilon \\ a^{q^2} b + ab^{q^2} &= \epsilon \\ a^{q^3} b + ab^{q^3} &= 0, \end{aligned}$$

where $d \in \mathbb{F}_4$, $\epsilon \in \mathbb{F}_4 \backslash \{0\}$ and $d \neq \epsilon$.

As $a, b \in \mathbb{F}_{q^3}$, we have

$$\epsilon_{i+3} = \begin{cases} a^{q^i} b + ab^{q^i} = ab + ba = 0 & \text{if } i \equiv 0 \bmod 3 \\ a^{q^i} b + ab^{q^i} = a^q b + ab^q = \epsilon & \text{if } i \equiv 1 \bmod 3 \\ a^{q^i} b + ab^{q^i} = a^{q^2} b + ab^{q^2} = \epsilon & \text{if } i \equiv 2 \bmod 3 \end{cases}$$

for $i \geq 1$, that is, (3.2) is satisfied. Moreover (3.4) is satisfied since $3|k = 2m$.

Hence, $\mathrm{Tr}(cx)^2 + \mathrm{Tr}(ax)\mathrm{Tr}(bx) = \mathrm{Tr}(xR(x))$ is a form of codimension 2 radical and invariant 0.

– Assume that $\epsilon = d$.

Using Lemma 3.1.11 we can find $a, b \in \mathbb{F}_{q^3}$ linearly independent over $\mathbb{F}_q$ such that

$$\begin{aligned} ab &= d \\ a^q b + ab^q &= d \\ a^{q^2} b + ab^{q^2} &= d \\ a^{q^3} b + ab^{q^3} &= 0, \end{aligned}$$

where $d \in \mathbb{F}_4 \backslash \{0\}$. As $a, b \in \mathbb{F}_{q^3}$, similar to the above case (3.2) and (3.4) is satisfied.

Hence, $\mathrm{Tr}(ax)\mathrm{Tr}(bx) = \mathrm{Tr}(xR(x))$ is a form of codimension 2 radical and invariant 1.

Case 3. Assume that $5|k$ and $R = \epsilon_0 x + A_5(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_1; x)$, where $\epsilon_0 \in \mathbb{F}_4$ and $\epsilon_1, \epsilon_2 \in \mathbb{F}_4 \backslash \{0\}$ with $\epsilon_1 \neq \epsilon_2$.

In this case we have the following three subcases depending on the invariant of R.

– Assume that one of the following holds: $\epsilon_0 = 0$ or $\epsilon_0 = \epsilon_1$ or $\epsilon_0 = \epsilon_2$.

Let $t = 2 \cdot 5^n t_0$ for some positive integers n and t_0 with $\gcd(5, t_0) = 1$. Set $v = 4^{5^n}$ so that $q = v^{t_0}$. Let y be a root of the polynomial f_v defined in (3.15). Then by Lemma 3.1.13 (part 1.) $y \in \mathbb{F}_{v^5} \subseteq \mathbb{F}_{q^5} \subseteq \mathbb{F}_{q^k}$. Set $a = y^v$, $b = y$ and $c = c_1 + c_2(a + b)$ with $c_1 \in \mathbb{F}_4 \backslash \{0\}$ and $c_2 \in \mathbb{F}_4 \backslash \{0, 1\}$.

Now, we first show that a, b, c are independent over $\mathbb{F}_q$. If not then c_1 is in the $\mathbb{F}_q$-span of a and b, that is, 1 is in the $\mathbb{F}_q$-span of a and b. Hence $a = gb + h$ for some $g, h \in \mathbb{F}_q$. That is, $y^v = gy + h$. Then using Lemma 3.1.13 (part 2.) we obtain

$$\begin{aligned} 0 &= y^{2v} + de^2 y^{v+1} + y^2 + d^2 e^2 \\ &= (gy + h)^2 + de^2(gy + h)y + y^2 + d^2 e^2 \\ &= y^2(g^2 + de^2 g + 1) + yde^2 h + (d^2 e^2 + h^2), \end{aligned} \tag{3.49}$$

where $e, d \in \mathbb{F}_4 \backslash \{0\}$ and $e \neq d$. Now, $y \notin \mathbb{F}_v$ by Lemma 3.1.13 (part 1.), and so has degree 5 over $\mathbb{F}_v$. As $\gcd(5, t_0) = 1$, y has degree 5 over $\mathbb{F}_q = \mathbb{F}_{v^{t_0}}$ as well. Thus $1, y, y^2$ are independent over $\mathbb{F}_q$. Then (3.49) gives $de^2 h = 0$, which means

$h = 0$, and $d^2e^2 + h^2 = 0$, that is, $h = de \in \mathbb{F}_4 \backslash \{0\}$, a contradiction. Thus a, b, c are independent over $\mathbb{F}_q$.

Now, we compute

$$\begin{aligned} c^2 + ab &= c_1^2 + c_2^2 y^{2v} + c_2^2 y^2 + y^{v+1} \\ &= c_1^2 + c_2^2 d^2 e^2 + (de^2 c_2^2 + 1) y^{v+1} \text{ by Lemma 3.1.13 (part 2.)} \\ &= c_1^2 + c_2^2 d^2 e^2 \text{ by Table 3.2.} \end{aligned}$$

Table 3.2: Some equalities in $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ where α is a root of the primitive polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$.

d	e	c_2	c_1	$c_1^2 + c_2^2 d^2 e^2$	d^2e^2	$de^2c_2^2 + 1$
1	α	α^2	1	0	α^2	0
			α	α	α^2	0
			α^2	α^2	α^2	0
	α^2	α	1	0	α	0
			α	α	α	0
			α^2	α^2	α	0
α	1	α	1	α^2	α^2	0
			α	1	α^2	0
			α^2	0	α^2	0
	α^2	α^2	1	α^2	1	0
			α	1	1	0
			α^2	0	1	0
α^2	1	α^2	1	α	α	0
			α	1	α	0
			α^2	0	α	0
	α	α	1	α	1	0
			α	1	1	0
			α^2	0	1	0

If $t_0 \equiv 1 \mod 5$ then we have $y^q = y^v$ and

$$\begin{aligned} a^q b + ab^q &= y^{v^2+1} + y^{2v} = d^2e^2 \text{ by Lemma 3.1.13 (part 3.)} \\ a^{q^2} b + ab^{q^2} &= y^{v^3+1} + y^{v^2+v} = e \text{ by Lemma 3.1.13 (part 4.)} \end{aligned}$$

Similarly using Lemma 3.1.13 we get the following results:

If $t_0 \equiv 2 \mod 5$ then we have $y^q = y^{v^2}$ and

$$\begin{aligned} a^q b + ab^q &= e \\ a^{q^2} b + ab^{q^2} &= d^2e^2. \end{aligned}$$

If $t_0 \equiv 3 \mod 5$ then we have $y^q = y^{v^3}$ and

$$\begin{aligned} a^q b + ab^q &= e \\ a^{q^2} b + ab^{q^2} &= d^2 e^2. \end{aligned}$$

If $t_0 \equiv 4 \mod 5$ then we have $y^q = y^{v^4}$ and

$$\begin{aligned} a^q b + ab^q &= d^2 e^2 \\ a^{q^2} b + ab^{q^2} &= e. \end{aligned}$$

As $a, b \in \mathbb{F}_{q^5}$, and using $\epsilon_1 = \epsilon_1^{q^4} = \epsilon_4$ and $\epsilon_2 = \epsilon_2^{q^3} = \epsilon_3$ we have

$$\epsilon_{i+5} = \begin{cases} a^{q^i} b + ab^{q^i} = ab + ba = 0 & \text{if } i \equiv 0 \bmod 5 \\ a^{q^i} b + ab^{q^i} = a^q b + ab^q = \epsilon_1 & \text{if } i \equiv 1 \bmod 5 \\ a^{q^i} b + ab^{q^i} = a^{q^2} b + ab^{q^2} = \epsilon_2 & \text{if } i \equiv 2 \bmod 5 \\ a^{q^i} b + ab^{q^i} = a^{q^3} b + ab^{q^3} = \epsilon_3 = \epsilon_2 & \text{if } i \equiv 3 \bmod 5 \\ a^{q^i} b + ab^{q^i} = a^{q^4} b + ab^{q^4} = \epsilon_4 = \epsilon_1 & \text{if } i \equiv 4 \bmod 5 \end{cases}$$

for $i \geq 1$, that is, (3.2) is satisfied. Moreover (3.4) is satisfied since $5|k = 2m$.

Hence, $\mathrm{Tr}(cx)^2 + \mathrm{Tr}(ax)\mathrm{Tr}(bx) = \mathrm{Tr}(xR(x))$ is a form of codimension 2 radical and invariant 0.

– Assume that $\epsilon_0 \neq 0$, $\epsilon_0 \neq \epsilon_1$, $\epsilon_0 \neq \epsilon_2$.

Let $q = 4^r$ with r is odd. Let v and y be as in the previous case. Now take $a = de^2 y^v$ and $b = d^2 ey$ which are independent over $\mathbb{F}_q$, and we can pick $s = de^2$ as our element of $\mathbb{F}_q$ with absolute trace 1. Note that $s \in \mathbb{F}_4 \backslash \{0, 1\}$ from the definition of f_v in (3.15).

Now, using Lemma 3.1.13 as in the previous case, we get

$$\begin{aligned} a^2 + ab + sb^2 &= d \\ a^q b + ab^q &= \begin{cases} d^2 e^2, & \text{if } t_0 \equiv 1 \text{ or } 4 \mod 5 \\ e, & \text{if } t_0 \equiv 2 \text{ or } 3 \mod 5. \end{cases} \\ a^{q^2} b + ab^{q^2} &= \begin{cases} e, & \text{if } t_0 \equiv 1 \text{ or } 4 \mod 5 \\ d^2 e^2, & \text{if } t_0 \equiv 2 \text{ or } 3 \mod 5. \end{cases} \end{aligned}$$

As $a, b \in \mathbb{F}_{q^5}$, similar to the above case (3.2) and (3.4) is satisfied.

Hence, $\mathrm{Tr}(ax)^2 + \mathrm{Tr}(ax)\mathrm{Tr}(bx) + \mathrm{Tr}(bx)^2 = \mathrm{Tr}(xR(x))$ is a form of codimension 2 radical and invariant -1.

– Assume that $e_0 \neq 0$, $e_0 \neq e_1$, $e_0 \neq e_2$.

Let $q = 4^r$ with r is an even integer. Using Lemma 3.1.12 we can find $a, b \in \mathbb{F}_{q^5}$ linearly independent over $\mathbb{F}_q$ such that

$$\begin{aligned} ab &= \alpha_0, \\ a^q b + ab^q &= \alpha_1, \\ a^{q^2} b + ab^{q^2} &= \alpha_2, \end{aligned}$$

where $\alpha_0, \alpha_1, \alpha_2 \in \mathbb{F}_4 \backslash \{0\}$ and all are different. As $a, b \in \mathbb{F}_{q^5}$, similar to the above case (3.2) and (3.4) is satisfied.

Hence, $\mathrm{Tr}(ax)\mathrm{Tr}(bx) = \mathrm{Tr}(xR(x))$ is a form of codimension 2 radical and invariant 1.

The above three cases complete the second part of the proof, which completes the proof.

■

3.3 Applications

In this section we use the results of Theorem 3.2.1 to obtain Artin-Schreier curves with many rational points. We use the notations and definitions related to Artin-Schreier curves as in [35] and for details we refer to [35].

Recall that $k = 2m$. Let $R(x) = \epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_{m-1} x^{q^{m-1}} \in \mathbb{F}_{q^k}[x]$ be an $\mathbb{F}_q$-linearized polynomial, with $\epsilon_i \in \mathbb{F}_4$, $0 \leq i \leq m-1$. The corresponding quadratic form is given by

$$Q_R(x) = \mathrm{Tr}\left(xR(x)\right).$$

Let $N(k)$ denote the cardinality

$$\begin{aligned} N(k) &= \left|\left\{x \in \mathbb{F}_{q^k} \mid Q_R(x) = 0\right\}\right| \\ &= \left|\left\{x \in \mathbb{F}_{q^k} \mid \mathrm{Tr}\left(xR(x)\right) = 0\right\}\right|. \end{aligned}$$

Let χ be the smooth, geometrically irreducible projective curve defined over $\mathbb{F}_{q^k}$ which is given by the plane affine equation

$$y^q - y = xR(x). \tag{3.50}$$

It is well known that the genus g of χ is (see [35, Proposition III.7.10])

$$g(\chi) = \frac{(q-1)\, q^{m-1}}{2},$$

where q^{m-1} is the degree of the $\mathbb{F}_q$-linearized polynomial $R(x)$.

Let $N(\chi)$ denote the number of $\mathbb{F}_{q^k}$-rational points of χ in (3.50). It is well known that using Hilbert's Theorem 90 (cf. [26, Theorem 2.25]) we have that

$$N(\chi) = 1 + qN(k). \tag{3.51}$$

Furthermore, the Hasse-Weil inequality states that

$$|N(\chi) - 1 - q^k| \leq 2g(\chi)q^{\frac{k}{2}}.$$

The curves attaining this bound are called maximal or minimal curves. If the number of $\mathbb{F}_{q^k}$-rational points of the curve is $1 + q^k + 2g(\chi)q^{\frac{k}{2}}$ or $1 + q^k - 2g(\chi)q^{\frac{k}{2}}$ then it is called maximal or minimal respectively. Clearly, to have a maximal or minimal curve $q^{\frac{k}{2}}$ should be an integer.

Now using the results obtained in the previous section we have the following theorems.

Theorem 3.3.1 *Let $k = 2m$ for some positive integer m. Then the curve (3.50) is maximal if and only if one of the following holds*

1. *$q = 4^r$ for some positive odd integer r, $4|k$ and $R(x) = dx + A_2(\epsilon; x)$ with $d, \epsilon \in \mathbb{F}_4 \setminus \{0\}$ and $d \neq \epsilon$,*

2. *$3|k$ and $R(x) = \epsilon x + A_3(\epsilon, \epsilon; x)$ with $\epsilon \in \mathbb{F}_4 \setminus \{0\}$,*

3. *$q = 4^r$ for some positive even integer r, $5|k$ and $R(x) = dx + A_5(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_1; x)$ with $d, \epsilon_1, \epsilon_2 \in \mathbb{F}_4 \setminus \{0\}$ and $d, \epsilon_1, \epsilon_2$ are all different.*

Proof. Note that $k = 2m$ and $R(x) = \epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_{m-1} x^{q^{m-1}} \in \mathbb{F}_{q^k}[x]$ and therefore degree of $R(x)$ is q^{m-1}.

Then the curve (3.50) is maximal if and only if

$$N(\chi) = 1 + qN(k) = 1 + q^k + 2g(\chi)q^{\frac{k}{2}}, \tag{3.52}$$

which implies that

$$\begin{aligned} N(k) &= q^{k-1} + 2g(\chi)q^{\frac{k}{2}-1} \\ &= q^{k-1} + 2g(\chi)q^{m-1} \\ &= q^{k-1} + 2\left(\frac{(q-1)\,q^{m-1}}{2}\right)q^{m-1} \\ &= q^{k-1} + (q-1)q^{k-2}. \end{aligned}$$

So by using

$$N(k) = q^{k-1} + \Lambda(Q_R)(q-1)q^{\frac{k+w}{2}-1},$$

we see that (3.52) holds if and only if $\Lambda(Q_R) = 1$ and $q^{\frac{k+w}{2}-1} = q^{k-2}$, that is $w = k-2$. Then by using Theorem 3.2.1 and Table 3.1 we get the desired results. ■

Theorem 3.3.2 *Let $k = 2m$ for some positive integer m. Then the curve (3.50) is minimal if and only if one of the following holds*

1. *$q = 4^r$ for some positive odd integer r, $4|k$ and $R(x) = dx + A_2(\epsilon; x)$ with $\epsilon \in \mathbb{F}_4 \setminus \{0\}$ and $d = 0$ or $d = \epsilon$,*
2. *$q = 4^r$ for some positive even integer r, $4|k$ and $R(x) = dx + A_2(\epsilon; x)$ with $\epsilon \in \mathbb{F}_4 \setminus \{0\}$,*
3. *$q = 4^r$ for some positive odd integer r, $5|k$ and $R(x) = dx + A_5(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_1; x)$ with $d, \epsilon_1, \epsilon_2 \in \mathbb{F}_4 \setminus \{0\}$ and $d, \epsilon_1, \epsilon_2$ are all different.*

Proof. Similar to the proof of Theorem 3.3.1 we observe that the curve (3.50) is minimal if and only if $\Lambda(Q_R) = -1$ and $w = k-2$. Then by using Theorem 3.2.1 and Table 3.1 we get the desired results. ■

REFERENCES

[1] S. Boztas, R. Hammons and P. V. Kumar, 4-phase sequences with near-optimum correlation properties. *IEEE Trans. Inf. Theory*, vol. 38, pp. 1101-1113, (1992).

[2] S. Boztas and P. V. Kumar, Binary sequences with Gold-like correlation but larger linear span, *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 532-537, Mar. (1994).

[3] E. Çakçak and F. Özbudak, Some Artin-Schreier type function fields over finite fields with prescribed genus and number of rational places, *J. Pure Appl. Algebra*, vol. 210, no. 1, pp. 113-135, (2007).

[4] J. H. Chung, and K. Yang, New design of quaternary low-correlation zone sequence sets and quaternary hadamard matrices, *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3733-3737, Aug. (2008).

[5] C. Ding, A. Salomaa, P. Sole and X. Tian, Three constructions of authentication secrecy codes, *J. Pure Appl. Algebra*, vol. 196, pp. 149–168, (2005).

[6] R. W. Fitzgerald, Highly Degenerate Quadratic Forms over finite fields of characteristic 2, *Finite Fields Appl.*, vol. 11, pp. 165-181, (2005).

[7] R. W. Fitzgerald, Highly Degenerate Quadratic Forms over F_2, *Finite Fields Appl.*, vol. 13, pp. 778-792, (2007).

[8] R. De Gaudenzi, C. Elia, and R. Viola, Bandlimited quasisynchronous CDMA: A novel satellite access technique for mobile and personal communication systems, *IEEE J. Sel. Areas Commun.*, vol. 10, no. 2, pp. 328-343, Feb. (1992).

[9] G. van der Geer, M. van der Vlugt, Quadratic forms, generalized Hamming weights of codes and curves with many points, *J. Number Theory*, vol. 59, pp. 20-36, (1996).

[10] R. Gold, Maximal recursive sequences with 3-valued recursive crosscorrelation functions, *IEEE Trans. Inf. Theory*, vol. 14, pp. 154-156, Jan. (1968).

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

[12] G. Gong, S. W. Golomb and H. -Y. Song, A note on low-correlation zone signal sets, *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2575-2581, Jul. (2007).

[13] B. Gordon, W. H. Mills, and L. R. Welch, Some new different sets, *Can. J. Math.*, vol. 14, pp. 614-625, (1962).

[14] J.-W. Jang, J.-S. No and H. Chung, A new construction of optimal p^2-ary lowcorrelation zone sequences using unified sequences, *IEICE Trans. Fundam.*, vol. E89-A, pp. 2656-2661, Oct. (2006).

[15] J.-W. Jang, J.-S. No, H. Chung, and X. H. Tang, New sets of optimal p-ary low-correlation zone sequences, *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 815-821, Feb. (2007).

[16] W.F. Jiang, L. Hu, X.H. Tang and X.Y. Zeng, New optimal quadriphase sequences with larger linear span, *Proc. ITW2007*, pp.57-61, Bergen, Norway, July (2007).

[17] T. Kasami, Weight enumerators for several classes of subcodes of the 2nd order Reed-Muller codes, *Information and Control*, vol. 18, pp. 369-394, (1971).

[18] E. L. Key, An analysis of the structure and complexity of nonlinear binary sequence generators, *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 732-736, Nov. (1976).

[19] K. Khoo, G. Gong and D.R. Stinson, New family of Gold-like sequences, *Proc. IEEE Inter. Symp. on Inf. Theory 02*, pp. 181., (2002)

[20] S.-H. Kim, J.-W. Jang, J.-S. No and H. Chung, New constructions of quaternary low correlation zone sequences, *IEEE Trans. Inf. Theory*, vol. 51, pp. 1469-1477, Apr. (2005).

[21] Y.-S. Kim, J.-W. Jang, J.-S. No, and H. Chung, New design of low correlation zone sequence sets, *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4607-4616, Oct. (2006).

[22] S. H. Kim and J. S. No, New families of binary sequences with low correlation, *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 3059-3065, Nov. (2003).

[23] A. Klapper, Cross-Correlations of Geometric Sequences in Characteristic Two, *Des. Codes Cryptogr.*, vol. 3 No. 4, pp. 347-377, (1993).

[24] A. Klapper, Cross-correlations of quadratic form sequences in odd characteristic, *Des. Codes Cryptogr.*, vol. 11, no. 3, pp. 289-305, (1997).

[25] V. I. Levenshtein, Bounds for codes as solutions of extremum problems for system of orthogonal polynomials, AAECC-93, *Lect. Note in Comput. Sci.*, vol. 673, Berlin: Springer-Verlag, pp. 25-42, (1993).

[26] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, (1997).

[27] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of applied cryptography*, Boca Raton: CRC Press, (1997).

[28] H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, Cambridge Univ. Press, Cambridge, (2001).

[29] F. Özbudak and Z. Saygı, Systematic Authentication Codes Using Additive Polynomials, *Des. Codes Cryptogr.*, vol 49, No. 1-3, pp. 61-77 (2008).

[30] E. K. Özbudak, F. Özbudak and Z. Saygı, A Class of Authentication Codes with Secrecy, Proceedings of International Workshop on Coding and Cryptography, pp. 273-285, May 10-15, (2009), Ullensvang, Norway.

[31] E. K. Özbudak, F. Özbudak and Z. Saygı, Artin-Schreier Type Curves and Quadratic Forms, Submitted.

[32] V. M. Sidelnikov, On mutual correlation of sequences, *Soviet Math. Dokl.*, vol.12, pp. 197-201, (1971).

[33] M. K. Simon, J. Omura, R. Scholtz and K. Levitt, *Spread Spectrum Communications*, vols. I-III. Computer Science Press, Rockville, (1985).

[34] P. Solé, A quaternary cyclic code, and a family of quadriphase sequences with low correlation properties. *Lect. Note Comput. Sci.*, vol. 388, pp. 193-201, (1989).

[35] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, (1993).

[36] X. H. Tang and P. Z. Fan, A class of pseudonoise sequences over GF(p) with low correlation zone, *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1644-1649, May (2001).

[37] X. H. Tang, P. Z. Fan, and S. Matsufuji, Lower bounds on correlation of spreading sequence set with low or zero correlation zone, *Electron. Lett.*, vol. 36, no. 6, pp. 551-552, Mar. (2000).

[38] X. Tang, T. Helleseth and P. Fan, A new optimal quaternary sequence family of length $2(2^n - 1)$ obtained from the orthogonal transformation of Families B and C, *Des. Codes Cryptogr.*, vol. 53, pp. 137-148, (2009).

[39] X.H. Tang, T. Helleseth, L. Hu and W.F. Jiang, A new family of Gold-like sequences, *Workshop of Sequences, Subsequences and Consequences*, University of Southern California, Los Angeles, California, USA, May-June (2007).

[40] X. H. Tang and P. Udaya, New construction of low correlation zone sequences from Hadamard matrices, *Proc. IEEE Inter. Symp. Inf. Theory*, Adelaide, Australia, pp. 482-486, Sep. 4-9 (2005).

[41] X. H. Tang and P. Udaya, New recursive construction of low correlation zone sequences, *Proc. 2nd Int. Workshop Sequence Design Appl. Commun.*, Shimonoseki, Japan, pp. 86-89, Oct. 10-14, (2005).

[42] X.H. Tang and P. Udaya, A note on the optimal quadriphase sequences families, *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 433-436, Jan. (2007).

[43] M. A. Tsfasman and S. G. Vladut, *Algebraic-Geometric Codes*, Kluwer, Dordrecht (1991).

[44] P. Udaya, *Polyphase and frequency hopping sequences obtained from finite rings*, Ph.D dissertation, Dept. Elec. Eng., Indian Inst. Technol., Kanpur, (1992).

[45] P. Udaya and M. U. Siddiqi, Optimal and suboptimal quadriphase sequences derived from maximal length sequences over $\mathbb{Z}_4$, *J. Appl. Algebra Eng. Commun*, vol. 9, pp. 161-191, (1998).

[46] L. R. Welch, Lower bounds on the maximum cross correlation of the signals, *IEEE Trans. Inf. Theory*, IT-20, pp. 397-399, May (1974).

[47] Z. Zhou, X. Tang and G. Gong, A new class of sequences with zero or low correlation zone based on interleaving technique, *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 4267-4273, Sept. (2008).

VITA

Elif Saygı graduated from Süleyman Demirel Science High School in 1997 and she received the B.Sc. degree in Mathematics from Middle East Technical University in 2002. She got her M.Sc. degree in Cryptography at Middle East Technical University in 2004. She has been working at Hacettepe University in Faculty of Education, since 2004. Her research interests include Boolean functions, stream ciphers, cryptography, finite fields, sequences.

She is married and she has a son and a daughter.

Publications

1. F. Özbudak, E. Saygı and Z. Saygı, Highly Degenerate Quadratic Forms over $\mathbb{F}_{2^k}$, to be submitted.

2. F. Özbudak, E. Saygı and Z. Saygı, Constructions of low correlation zone sequence sets, to be submitted.

3. A. Doğanaksoy, E. Saygı and Z. Saygı, Some Necessary Conditions for a Quadratic Feedback Shift Register to Generate a Maximum Length Sequence, *BFCA 2007, Proceedings of Third International Workshop on Boolean Functions : Cryptography and Applications*, May 2-3, (2007), Paris, France.

4. A.Doğanaksoy and E. Saygı, Quadratic Feedback Shift Registers Generating Maximum Length Sequemces, *II. Ulusal Kriptoloji Sempozyumu Bildiriler Kitabı*, pp. 141-145, December 15-17, (2006), Ankara, TURKEY.

5. E. Saygı, Z. Saygı, M. S. Turan and A. Doğanaksoy, Statistical approach on the number of SAC satisfying functions, *BFCA 2005, Proceedings of First International Workshop on Boolean Functions: Cryptography and Applications*, pp. 39-48, March 7-9, (2005), Rouen, France.

6. A.Doğanaksoy and E. Saygı, On the Quadratic Feedback Shift Registers, *I. Ulusal Kriptoloji Sempozyumu Bildiriler Kitabı*, pp. 127-133, November 18-20, (2005), Ankara, TURKEY.