# A Note on Low Correlation Zone Signal Sets

Guang Gong[1], Solomon W. Golomb[2], and Hong-Yeop Song[3⋆]

[1] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario N2L3G1, CANADA, ggong@calliope.uwaterloo.ca
[2] Department of EE-SYSTEMS, University of Southern California, Los Angeles, CA, 90089-2565, USA, milly@usc.edu
[3] Center for Information Technology of Yonsei University, Coding and Information Theory Lab, Department of Electrical and Electronics Engineering, Yonsei University, Seoul, 120-749, Korea, hysong@yonsei.ac.kr

**Abstract.** In this note, we present a connection between designing low correlation zone (LCZ) sequences and the results of correlation of sequences with subfield decompositions presented in a recent book by the first two authors [2]. This results in low correlation zone signal sets with huge sizes over three different alphabetic sets: finite field of size $q$, integer residue ring modulo $q$, and the subset in the complex field which consists of powers of a primitive $q$-th root of unity. We also provide two open problems along this direction.

**Index Terms:** low correlation zone sequences, subfield reducible sequences, two-tuple balance property.

## 1 Introduction

Recently, there have been some interesting developments involving quasi-synchronous (QS) CDMA communication systems and on the design of sequences with low correlation zone (LCZ) that can be used in such systems [1][8][9][5].

This paper will describe a general approach to the design of LCZ sequences using the results on sequences with subfield decompositions, presented in Chapter 8 of [2] by the first two authors [2]. The above known cited results on LCZ sequences can be obtained easily from this general setting.

### 1.1 Notation

We use the following notation throughout the paper.

⋆ He is supported by grant No.(R01-2003-000-10330-0) from the Basic Research Program of the Korea Science & Engineering Foundation

- The finite field $GF(q^n)$ is denoted by $\mathbb{F}_{q^n}$ for any positive integer $n$ and $q = p^t$, a power of a prime, and the multiplicative group of $\mathbb{F}_{q^n}$ is denoted by $\mathbb{F}_{q^n}^*$.
- The trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^m}$ where $m$ is a factor of $n$, i.e., $m|n$, is denoted by $Tr_m^n(x) = x + x^Q + \cdots + x^{Q^{l-1}}$ where $Q = q^m$ and $n = lm$. If the context is clear, we drop the subscript and superscript of $Tr_1^n(x)$, i.e., we write $Tr_1^n(x)$ as $Tr(x)$ for simplicity.
- $\alpha$ always denotes a primitive element of $\mathbb{F}_{q^n}$.
- Let $\{a_i\}$ be a sequence over $\mathbb{F}_q$ of period $q^n - 1$. Using the (discrete) Fourier transform, there exists a function $f(x)$ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ such that $a_i = f(\alpha^i), i = 0, 1, \cdots$, which can be written as a sum of monomial trace terms. We say that $f(x)$ is a trace representation of $\mathbf{a}$ associated with $\alpha$, or $\mathbf{a}$ is an evaluation of $f(x)$ (for details, see [2]). For any function $f(x)$ appearing in this paper, we assume that $f(0) = 0$ if there is no other specification. For each function $f(x)$ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, there is a boolean representation in $n$ variables for $f(x)$, denoted by $f(\mathbf{x}) = f(x_1, \cdots, x_n)$ where $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{F}_q^n$. Since $\mathbb{F}_{q^n}$ is isomorphic to $\mathbb{F}_q^n$, we identify the elements of $\mathbb{F}_{q^n}$ as vectors in $\mathbb{F}_q^n$ if this is useful. We also use the terms a function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ and a boolean function in $n$ variables over $\mathbb{F}_q$ (i.e., a function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$) interchangeably.
- Let $\{\alpha_i\}$ be a self-dual basis of $\mathbb{F}_{q^n}$. Let $x = x_1\alpha_1 + \cdots + x_n\alpha^n \in \mathbb{F}_{q^n}, x_i \in \mathbb{F}_q$ and $y = y_1\alpha_1 + \cdots + y_n\alpha^n \in \mathbb{F}_{q^n}, y_i \in \mathbb{F}_q$. Then $\mathbf{x} \cdot \mathbf{y} = Tr_1^n(xy)$ where $\mathbf{x} = (x_1, \cdots, x_n)$ and $\mathbf{y} = (y_1, \cdots, y_n)$ and $\mathbf{x} \cdot \mathbf{y} = \sum_i^n x_i y_i$, the dot product of $\mathbf{x}$ and $\mathbf{y}$.

### 1.2 Three Types of Crosscorrelations

Let $N = q^n - 1$ and $\mathbf{a} = \{a_i\}$ and $\mathbf{b} = \{b_i\}$ be two sequences over $\mathbb{F}_q$ of period $q^n - 1$ where $q = p^t$ where $p$ is a prime. When $t > 1$ there seems to be no single (universally accepted or applicable) consensus on the correlation between $\mathbf{a}$ and $\mathbf{b}$. At least three different notions have been proposed [2], and we will use the following (see Question 16 in Exercises for Chapter 5 in [2]):

Let $\eta$ be a primitive $q$th root of unity, i.e., there is some integer $j$ such that $\eta = \exp(\frac{j2\pi}{q})$ with $\gcd(j, q) = 1$. Let $\{\alpha_0, \alpha_1, \cdots, \alpha_{t-1}\}$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$.

For $x \in \mathbb{F}_q$, we have

$$x = \sum_{i=0}^{t-1} x_i \alpha_i, x_i \in \mathbb{F}_p. \tag{1}$$

We define

$$\rho(x) = \sum_{i=0}^{t-1} x_i p^i, x_i \in \mathbb{F}_p. \tag{2}$$

Then $\rho$ shows a one-to-one correspondence between the finite field $\mathbb{F}_q$ and the integer residue ring $\mathbb{Z}_q$. If $q = p$, then $\rho(x) = x$. The crosscorrelation between $\mathbf{a}$ and $\mathbf{b}$ is defined as

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \begin{cases} \sum_{i=0}^{N-1} \eta^{a_{i+\tau} - b_i}, & q = p, \tau = 0, 1, \cdots \\ \sum_{i=0}^{N-1} \eta^{\rho(a_{i+\tau}) - \rho(b_i)}, & q = p^t, t > 1, \tau = 0, 1, \cdots. \end{cases} \tag{3}$$

In other words, the elements of $\mathbb{F}_{p^t}$ are represented by the $p$-adic numbers in $\mathbb{Z}_q$ as stated in [2].

From this definition, when $q = p^t$ for $t > 1$, we essentially obtain correlation of sequences whose elements are taken from three different alphabets.

(1) The crosscorrelation between $\mathbf{a} = \{a_i\}$ and $\mathbf{b} = \{b_i\}$, where $a_i, b_i \in \mathbb{F}_q$, i.e., the elements of the sequences $\mathbf{a}$ and $\mathbf{b}$ are taken from the finite field $\mathbb{F}_q$ with $q$ elements.

(2) Let

$$u_i = \rho(a_i) \in \mathbb{Z}_q, \text{ and } v_i = \rho(b_i) \in \mathbb{Z}_q, 0, 1, \cdots. \tag{4}$$

Through the definition of the crosscorrelation of $\mathbf{a}$ and $\mathbf{b}$, we obtain a crosscorrelation of $\mathbf{u} = \{u_i\}$ and $\mathbf{v} = \{v_i\}$ which are integer sequences over $\mathbb{Z}_q$. In other words, the crosscorrelation between $\mathbf{u}$ and $\mathbf{v}$ is given by

$$C_{\mathbf{u},\mathbf{v}}(\tau) = \sum_{i=0}^{N-1} \eta^{u_{i+\tau} - v_i}, \tau = 0, 1, \cdots. \tag{5}$$

(3) Let $\mathbf{s} = \{s_i\}$ and $\mathbf{t} = \{t_i\}$ whose elements are defined as

$$s_i = \eta^{u_i} = \eta^{\rho(a_i)} \text{ and } t_i = \eta^{v_i} = \eta^{\rho(b_i)}, i = 0, 1, \cdots, . \tag{6}$$

Thus $\mathbf{s}$ and $\mathbf{t}$ are sequences over the complex $q$-th roots of unity, i.e., in the complex field $\mathbb{C}$. The crosscorrelation between $\mathbf{s}$ and $\mathbf{t}$ is defined as

$$C_{\mathbf{s},\mathbf{t}}(\tau) = \sum_{i=0}^{N-1} s_{i+\tau} t_i^*, \ \tau = 0, 1, \cdots, \tag{7}$$

where $x^*$ means the conjugate of the complex number $x$.

The crosscorrelations of these three types of sequences are equal, i.e., we have

$$C_{\mathbf{a},\mathbf{b}}(\tau) = C_{\mathbf{u},\mathbf{v}}(\tau) = C_{\mathbf{s},\mathbf{t}}(\tau), \tau = 0, 1, \cdots. \tag{8}$$

Thus, if we derive the crosscorrelation between sequences over $\mathbb{F}_q$, then at the same time we obtain the crosscorrelation between sequences over $\mathbb{Z}_q$ and the crosscorrelation between sequences over the complex field, defined by (4) and (6), respectively. Therefore, all the results on correlation derived in this paper for sequences over $\mathbb{F}_q$ are valid for the other two classes of sequences.

In the rest of the paper, for simplicity, we will omit the map $\rho$ in correlation calculation, but it should understand that if $q = p^t, t > 1$, $x$ in $\eta^x, x \in \mathbb{F}_q$ represents the $p$-adic representation of $x$, i.e., $\rho(x)$ defined by (2).

We may write the correlation function $C_{\mathbf{a},\mathbf{b}}(\tau)$ in terms of exponential sums as follows, which can simplify proofs for correlation calculations in many cases.

$$C_{\mathbf{a},\mathbf{b}}(\tau) + 1 = \begin{cases} \sum_{x \in \mathbb{F}_{q^n}} \eta^{a(\lambda x) - b(x)}, & q = p \\ \sum_{x \in \mathbb{F}_{q^n}} \eta^{\rho(a(\lambda x)) - \rho(b(x))}, & q = p^t, t > 1 \end{cases} \tag{9}$$

where $\lambda = \alpha^\tau \in \mathbb{F}_{q^n}^*$, $a(x)$ and $b(x)$ are the trace representations of $\mathbf{a}$ and $\mathbf{b}$ respectively. (Note. Both $a(x)$ and $b(x)$ are functions from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$.) The equation (9), in fact, is the definition of the crosscorrelation between two functions $a(x)$ and $b(x)$ [2]. In other words, the crosscorrelation between $a(x)$ and $b(x)$, denoted by $C_{a,b}(\lambda)$, is defined as

$$C_{a,b}(\lambda) = \begin{cases} \sum_{x \in \mathbb{F}_{q^n}} \eta^{a(\lambda x) - b(x)}, & q = p \\ \sum_{x \in \mathbb{F}_{q^n}} \eta^{\rho(a(\lambda x)) - \rho(b(x))}, & q = p^t, t > 1. \end{cases} \tag{10}$$

Thus, the relationship of the correlation between the sequences $\mathbf{a}$ and $\mathbf{b}$ to the correlation between the functions $a(x)$ and $b(x)$ is given by

$$C_{\mathbf{a},\mathbf{b}}(\tau) + 1 = C_{a,b}(\lambda), \ \lambda = \alpha^\tau \in \mathbb{F}_{q^n}^*. \tag{11}$$

We will use the correlation of the function version for derivations in the rest of this paper.

### 1.3 LCZ and Almost LCZ Sequences

We now review the concept of sequences with low correlation zone (LCZ) and define "almost" LCZ sequences. Let $\mathbf{s}_j = (s_{j,0}, s_{j,1}, \cdots, s_{j,N-1}), 0 \leq j < r$, be $r$ shift-distinct sequences over $\mathbb{F}_q$ with period $N$. Let $S = \{\mathbf{s}_0, \mathbf{s}_1, \cdots, \mathbf{s}_{r-1}\}$. If for any two sequences in $S$, say $\mathbf{a}$ and $\mathbf{b}$, $C_{\mathbf{a},\mathbf{b}}(\tau)$, the correlation function between $\mathbf{a}$ and $\mathbf{b}$ defined by (3), satisfies $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leq \delta$, then $S$ is said to be an $(N, r, \delta)$ *signal set*, and $\delta$ is referred to as the *maximum correlation of* $S$. If we put a condition on the range of $\tau$, i.e., for a fixed nonnegative number $d$, if for any two sequences $\mathbf{a}$ and $\mathbf{b}$ in $S$, we have

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \leq \delta, \forall\, |\tau| < d \tag{12}$$

then $S$ is referred to as an $(N, r, \delta, d)$ *low correlation zone* (LCZ) signal set. Note that in communication practice, especially in the uplink of QS-CDMA systems, any received signal most likely has a phase shift, thus, the value of the crosscorrelation at $\tau = 0$ may not have significant effect during the detection process. Thus if the crosscorrelation of any two sequences in $S$ satisfies the following conditions:

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \leq \delta,\ \forall\, 0 < |\tau| < d \tag{13}$$

we call $S$ an $(N, r, \delta, d)$ *almost low correlation zone* (ALCZ) signal set.

According to this definition, if $d = \lceil N/2 \rceil$, then a $(N, r, \delta, d)$ LCZ signal set becomes a $(N, r, \delta)$ signal set. Recently, there have been several constructions of LCZ signal sets with parameters $(N, r, 1, d)$ where $d = \frac{q^n-1}{q^m-1}$, where $m|n$, and the values of $r$ depend on $m$ [8][9][5].

It is quite interesting to observe that all such LCZ signal sets come from a well-known fact which is presented in [2]. In the following section, we present this relation. In Section III, we give two open problems and some concluding remarks.

## 2 Crosscorrelation of Subfield Reducible Sequences

A function $f(x)$ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is said to be *balanced* if each element in $\mathbb{F}_q$ occurs in $\{f(x) \,|\, x \in \mathbb{F}_{q^n}\}$ exactly $q^{n-1}$ times. We set $Q = q^m$, $n = lm$, and $d = \frac{q^n-1}{q^m-1}$.

**Definition 1.** *Let $f(x)$ be a function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ with $f(0) = 0$ and let*

$$T_f(\lambda) = \{(f(x), f(\lambda x)) \,|\, x \in \mathbb{F}_{q^n}\}, \lambda \in \mathbb{F}_{q^n}. \tag{14}$$

*We say that $f(x)$ satisfies the* two-tuple balance property *if $f(x)$ satisfies the following two conditions:*

1. *For $\lambda \notin \mathbb{F}_Q$ each pair $(\theta, \mu) \in \mathbb{F}_Q^2$ occurs $Q^{l-2}$ times in $T_f(\lambda)$.*
2. *For $\lambda \in \mathbb{F}_Q^*$, the multiplicative group of $\mathbb{F}_Q$, there exists some $\mu \in \mathbb{F}_q$ such that $(\theta, \mu\theta)$ occurs $q^{n-1}$ times in $T_f(\lambda)$ for every $\theta \in \mathbb{F}_q$.*

**Definition 2.** (Gong and Golomb, 2002 [3][2]) *Let $\mathbf{u} = \{u_i\}$ be a sequence over $\mathbb{F}_q$ of period $N = q^n - 1$ with trace representation $u(x)$. If there is $m > 1$, a proper factor of $n$, such that $u(x)$ can be decomposed into a composition of $h(x)$ and $g(x)$ where $h(x)$ is a function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^m}$, and $g(x)$ a function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, i.e.,*

$$u(x) = g(x) \circ h(x) \tag{15}$$

*or in diagram form*

$$\begin{array}{c} \mathbb{F}_{q^n} \\ \downarrow \quad h(x) \\ \mathbb{F}_{q^m} \\ \downarrow \quad g(x) \\ \mathbb{F}_q \end{array}$$

*then we say that $u(x)$ or $\mathbf{u}$ is* subfield reducible, *(15) is called* a subfield factorization *of $u(x)$ or $\mathbf{u}$. Otherwise, $u(x)$ or $\mathbf{u}$ is said to be* subfield irreducible.

From this definition, we know that $m$-sequences of period $q^n - 1$ are subfield reducible if $n$ is not a prime. Note that the subfield reducibility or irreducibility of functions or sequences is meaningful only for $n$ composite.

In [2], it is shown that the autocorrelation of a subfield reducible sequence given by $a(x) = f(x) \circ h(x)$ where $h(x)$ is a function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^m}$ with the two-tuple balance property, and $f(x) : \mathbb{F}_{q^m} \to \mathbb{F}_q$ is balanced, is equal to $-1$ for all values of $\tau \not\equiv 0 \,(\mathrm{mod}\, d)$ and the autocorrelation of $a(x)$ for $\tau \equiv 0 \,(\mathrm{mod}\, d)$ is equal to the autocorrelation of $f(x)$ multiplied by a scalar factor. (Refer to Theorem 8.1 and Corollary 8.2 in [2] for details.) They also illustrated the effect of autocorrelation of this type of subfield reducible sequences using an example (Example 8.2 in [2]). In other words, there are only $q^m - 1$ autocorrelation values

at $\tau$'s which are multiples of $d$ which are undetermined. Compared to those $\tau$'s whose correlation values are equal to $-1$ (there are $q^n - q^m$ such $\tau$'s), the number of undetermined values is relatively quite small and these $\tau$ values are far from the origin (i.e., from $\tau = 0$) since they are multiples of $d = \frac{q^n-1}{q^m-1}$. This result and its proof has its origin rooted in calculating autocorrelation functions of GMW or generalized GMW sequences, geometrical sequences by Klapper, Chan and Goresky [7] and $k$-form sequences [6] in which $h(x)$ is a trace function $Tr_1^n(x^k)$, a cascaded GMW function, or a $k$-form function.

There is a similar result for the crosscorrelation between two such subfield sequences and the proof also can be given in a similar fashion to that for their autocorrelation functions. Unfortunately, this fact has not received sufficient publicity. We reproduce it here.

**Theorem 1.** *Let $h$ be a function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^m}$ with the two-tuple balance property, and $f$ and $g$ be* any *two functions from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Let $\mathbf{a}$ and $\mathbf{b}$ be two sequences over $\mathbb{F}_q$ with $a(x) = f(x) \circ h(x)$ and $b(x) = g(x) \circ h(x)$ as their trace representations, respectively. Let $\lambda = \alpha^\tau$. Then $C_{f\circ h, g\circ h}(\lambda)$, the crosscorrelation between $\mathbf{a}$ and $\mathbf{b}$, is given by*

$$C_{\mathbf{a},\mathbf{b}}(\tau) + 1 = C_{f\circ h, g\circ h}(\lambda)$$
$$= \begin{cases} Q^{l-2} \sum_{x\in\mathbb{F}_Q} \eta^{f(x)} \sum_{y\in\mathbb{F}_Q} \eta^{-g(y)}, \ \lambda \notin \mathbb{F}_q \quad or\ \tau \not\equiv 0 \pmod d \\ = Q^{l-1} C_{f,g}(\lambda), \qquad\qquad \lambda \in \mathbb{F}_q \quad or \ \ \tau = jd, j = 0, 1, \cdots. \end{cases}$$

*In particular, if one of the functions $f$ or $g$ is balanced, then*

$$C_{\mathbf{a},\mathbf{b}}(\tau) = C_{f\circ h, g\circ h}(\tau) - 1 = -1, \quad \forall \tau \not\equiv 0 \pmod d.$$

*Proof.* For $\lambda \neq 1$,

$$C_{f\circ h, g\circ h}(\lambda) = \sum_{x\in\mathbb{F}_{q^n}} \eta^{f(h(\lambda x)) - g(h(x))} \tag{16}$$

1. Assume $\lambda \notin \mathbb{F}_Q^*$ (recall $Q = q^m$). In this case, substituting Condition 1 of Definition 1 into (16), we have

$$\begin{aligned} C_{f\circ h, g\circ h}(\lambda) &= Q^{l-2} \sum_{\theta,\mu\in\mathbb{F}_Q} \eta^{f(\theta)-g(\mu)} \\ &= Q^{l-2} \sum_{\theta\in\mathbb{F}_Q} \eta^{f(\theta)} \sum_{\mu\in\mathbb{F}_Q} \eta^{-g(\mu)} \\ &\Longrightarrow C_{f\circ h, g\circ h}(\lambda) = 0 \ (\text{ if one of } f \text{ or } g \text{ is balanced}). \end{aligned}$$

2. Assume $0 \neq \lambda \in \mathbb{F}_Q$. Substituting Condition 2 of Definition 1 into (16), we have

$$\begin{aligned} C_{f\circ h, g\circ h}(\lambda) &= Q^{l-1} \sum_{\theta \in \mathbb{F}_Q} \eta^{f(\mu\theta)-g(\theta)}, 1 \neq \mu \in \mathbb{F}_{q^m} \\ &= Q^{l-1} C_{f,g}(\mu). \end{aligned}$$

For $\lambda \in \mathbb{F}_Q$, since $\beta = \alpha^d$ is a primitive element in $\mathbb{F}_Q$, we may write $\lambda = \beta^j = \alpha^{jd} \Longrightarrow \tau = jd$ which completes the proof.

□

Thus, for two subfield reducible sequences, given by $f \circ h$ and $g \circ h$ where $h$ satisfies the two-tuple balance property and one of $f$ and $g$ is balanced, then their crosscorrelation function takes the value $-1$ for all $\tau$'s which are not multiples of $d$; i.e., there are $q^n - q^m$ values of $\tau$ such that $C_{\mathbf{a},\mathbf{b}}(\tau) = C_{f\circ h, g\circ h}(\lambda) - 1 = -1$. There are only $q^m - 1$ values of $\tau$ remaining undetermined. These undetermined values depend on the crosscorrelation between $f$ and $g$, i.e., $C_{f\circ h, g\circ h}(\alpha^{id}) = q^{n-m} C_{f,g}(\beta^i), i = 0, 1, \cdots, q^m - 2$ where $\beta = \alpha^d$.

Observe that the condition that makes $C_{f\circ h, g\circ h}(\lambda) = 0$ for so many values of $\tau$ is rather weak, and it easily produces an almost LCZ signal set of gigantic size. Before we discuss the size, we need the following lemma whose proof is immediate from the balance property.

**Lemma 1.** *Let $U^-$ be a set consisting of all shift-distinct sequences over $\mathbb{F}_q$ with period $q^m - 1$ and the balanced property. Let $\mathcal{F}^-$ be a set consisting of functions from $F_{q^m}$ to $F_q$ with the balance property. Then an evaluation of any function in $\mathcal{F}^-$ is a sequence in $U^-$. Furthermore,*

$$|U^-| = \frac{|\mathcal{F}^-|}{q^m - 1}.$$

Applying this lemma, we have the following result.

**Theorem 2.** *Let $\Pi_0$ be the set consisting of all subfield reducible sequences with the trace representations $f \circ h$ where $h$ is a fixed function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^m}$ with the two-tuple balance property and the evaluation of $f$'s runs through $U^-$. Then*

1. *Any two sequences in $\Pi_0$ are shift-distinct.*

2. *For any two sequences in $\Pi_0$, say* $\mathbf{a}$ *and* $\mathbf{b}$*,*

$$C_{\mathbf{a},\mathbf{b}}(\tau) = -1, \forall\ \tau \not\equiv 0 \,(\mathrm{mod}\, d).$$

*Moreover, $\Pi_0$ is a $(N, r, 1, d)$ almost LCZ signal set where $r = |U^-|$.*

*Proof.* Let $f \circ h$ and $g \circ h$ be the trace representations of $\mathbf{a}$ and $\mathbf{b}$, respectively. Then $\mathbf{a}$ and $\mathbf{b}$ are shift-distinct if and only if the evaluations of $f$ and $g$ are shift-distinct (see details in Section 8.1 in [2]). Since any two sequences in $U^-$ are shift-distinct, then $\mathbf{a}$ and $\mathbf{b}$ are shift-distinct. The crosscorrelation property directly follows from Theorem 1. □

Here are a few remarks about Theorem 2.

1. The size of $\Pi_0$ is huge. Its lower bound is given by

$$r = |U^-| \geq \frac{(q-1)q^{q^{m-1}}}{q^m - 1}. \tag{17}$$

Note that $f(\mathbf{x}) = cx_1 + f_1(x_2, \cdots, x_m), c \in \mathbb{F}_q^*$ is a balanced function where $f_1(x_2, \cdots, x_m)$ is an arbitrary function of $m-1$ variables. There are $q-1$ ways to pick $c$ and $q^{q^{m-1}}$ ways to pick the function $f_1$. Thus the size of $\mathcal{F}^-$ is greater than the product of $(q-1)$ and $q^{q^{m-1}}$. By removing shift-equivalent sequences, we have (17).

2. For $q = p^t$ where $t > 1$, let $\Pi_1$ and $\Pi_2$ be the sets consisting of the sequences over $\mathbb{Z}_q$ transformed from $\Pi_0$ by (4) and the sequences over the complex field transformed from $\Pi_0$ by (6), respectively. Then both $\Pi_1$ and $\Pi_2$ are $(N, r, 1, d)$ almost LCZ signal sets.
3. Let $h(x) : \mathbb{F}_{q^n} \to \mathbb{F}_{q^m}$ which satisfies the following two conditions:
   (i) $h(x)$ is $k$-form, i.e., for any $\lambda \in \mathbb{F}_{q^m}^*$ and $x \in \mathbb{F}_{q^n}$, $h(\lambda x) = \lambda^k h(x)$, $\gcd(k, q^n - 1) = 1$.
   (ii) $h(x)$ has the difference balance property, i.e., for any $\lambda \in \mathbb{F}_{q^n}$, $\lambda \neq 1$, $h(x) - h(\lambda x)$ is balanced.

   In 2002 [4], Gong and Song established essentially the following result:

   **Fact 1** *If $h(x)$ is $k$-form then it has cyclic array structure. If, in addition, $h(x)$ has the difference balance property, then it has the two-tuple balance property.*

The known results on LCZ sequences come from the general construction for $\Pi_0$, in which either $h$ is a monomial trace term [8][9] for $q = 2$ or $q = p$, or $h$ satisfies both $k$-form and the difference balance property [5] for $q = 2^2$. In all this research, the results of Theorem 1 have been established repeatedly for different subsets of $U^-$ where these subsets have their respective sizes smaller than $q^m$. Note that the results of Theorem 1 are very easy to establish via exponential sums together with Fact 1.

Note that if $C_{f\circ h, g\circ h}(0) = 0$ or equivalently $C_{f,g}(0) = 0$, then $\Pi_0$ becomes a $(N, r_0, 1, d)$ LCZ signal set where $r_0$ is the size of the subset, say $K$, of $U^-$ which satisfies that the term-by-term difference of two shift-distinct sequences is still a balanced sequence.

## 3 A Construction of $K$

In the following section, we provide an important result on the achievable upper bound for the size of $K$, a connection between constructions of $K$ and the Hadamard matrices, and a construction for $K$ which achieves this upper bound. The following theorem gives a more general result about an upper bound size of $K$.

**Theorem 3.** *Suppose $K$ is a collection of balanced sequences over $\mathbb{F}_q$ of period $P$ (here we do not care whether or not they are shift distinct, and we do not have to restrict the value of $P$) such that the term-by-term difference of any two sequences in $K$ is again balanced. Then the size $|K|$ of $K$ (the number of sequences in $K$) cannot exceed $P$.*

*Proof.* In the following, we only give a proof for binary case, since the proof for the $q$-ary case is similar to that for the binary case. Note that the term-by-term difference of two binary sequences is the same as the term-by-term sum of these two sequences.

Use $+1$ and $-1$ as the two binary values, and consider the sequences in $K$ as vectors of length $P$, i.e. of dimension $P$. The "balanced sums" property says that the dot product of each pair of vectors is zero, so the vectors are orthogonal, and the number of mutually orthogonal vectors cannot exceed the dimension of

the vector space. (While this is the proof when $P$ is *even*, it is easily modified for odd $P$. If the dot product of each pair of vectors is always $-1$, add one extra component to each of the vectors, and give this extra component the same value for each vector, so we've added *one* to the dot products to make them all zero, and each vector should now be exactly balanced between $+1$'s and $-1$'s. Since the dimension is now $P+1$, it is possible to have $P+1$ mutually orthogonal vectors; but the "all 1's" vector is orthogonal to each of the others because they are balanced, and the "all 1's" vector is *not* balanced, leaving at most $P$ "balanced" vectors in the set $K$.)

□

**Corollary 1.** *Recall that $U^-$ denotes a set consisting of all the shift-distinct balanced sequences over $\mathbb{F}_q$ of period $q^m-1$, and let $K \subset U^-$ which is closed under the term-by-term differences of two sequences in it. That is, for any two sequences in $K$ their term-by-term difference is still balanced. Then the size $|K|$ of $K$ is upper bounded by $q^m-1$.*

*Proof.* This is the case of $P = q^m - 1$ in Theorem 3.

□

In this following, we show the relationship of the set $K$ and a $q$-ary Hadamard matrix.

Let $H = (h_{ij})_{v\times v}$ where $h_{ij} = \omega^{s_{ij}}, s_{ij} \in \mathbb{F}_q$ and $\omega$ is a primitive $q$th root of unity. $H$ is sai d to be a *Hadamard matrix* if $HH^* = vI_v$ where $H^* = (h_{ij}^*)$ where $x^*$ is the complex conjugation of $x$ and $I_v$ is the $v \times v$ identity matrix. In other words, $H$ is a Hadamard matrix if the inner (or Hermitian dot if $q > 2$) product of any two row vectors of $H$ is equal to zero or any two row vectors of $H$ are orthogonal.

Note that $H$ is symmetric and one of row vector of $H$ is a constant vector. Applying the elementary transforms to $H$, we can write $H$ as a matrix in which the first row so that the first column is the all one's vector up to a linear transformation. Let $v = q^m$. Let $H^-$ denote the matrix resulting from $H$ by deleting the first column and the first row. We say that $H^-$ is the reduced form of $H$. From the definition of the Hadamard matrices and Theorem 2, the following result is immediate.

**Proposition 1.** *With the above notation, assume that $H$ be a $q^m \times q^m$ matrix over $\mathbb{F}_q$, and let $g_j(\alpha^i) = s_{ij}$ where $h_{ij} = \omega^{s_{ij}}, s_{ij} \in \mathbb{F}_q$ and $\alpha$ is a primitive element of $\mathbb{F}_{q^m}$. Let $K$ be a set consisting of the sequences whose trace representations are $g_j$'s, $1 \leq j < q^m\}$. Then $K$ produces a LCZ signal set with parameters $(N, r_0, 1, d)$ if and only if $H$ is a Hadamard matrix. Furthermore, $r_0 = q^m - 1$ if and only if any two rows of $H^-$ are shift distinct when they are considered as sequences.*

Therefore, the classification of all LCZ signal sets with parameters $(N, q^m - 1, 1, d)$ by the subfield decomposition construction (Theorem 2) is equivalent to the classification of all $q^m \times q^m$ Hadamard matrices for which row vectors in the reduced forms are shift distinct. For these $K$'s, the sizes of $K$ achieves the maximum values.

Note that for the known constructions, $|K| < q^{m-1}$ for $q = p$ [9] and $|K| = q^{m/2}$ for $q = 2^2$ [5].

In the following, we give a construction for $K$ in which the size $|K|$ of $K$ achieves the upper bound $q^m - 1$. For the construction given below, the case of $q = 2$ has a much simpler proof. However, the proof for $q > 2$ cannot be obtained from the case of $q = 2$ by simply replacing 2 by $q$, as Theorem 3. So, we will directly proceed it for a general $q$.

Before we give a construction for $K$, we present the following result on balanced functions.

**Lemma 2.** *Let $m = s + r$, $h(x)$ be a function from $\mathbb{F}_q^s$ to $\mathbb{F}_q^r$ with $h(x) \neq 0$ for all $x \in \mathbb{F}_q^s$, $\Phi(y)$ is a permutation of $\mathbb{F}_q^s$, and $t(x)$ is an arbitrary function from $\mathbb{F}_q^s$ to $\mathbb{F}_q$. Then $f(x, y) = h(x) \cdot \Phi(y) + t(x)$ is a balanced function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.*

*Proof.* Since $\Phi(y)$ is a permutation of $\mathbb{F}_q^r$, for a fixed nonzero element $a \in \mathbb{F}_q^r$, any element in $\mathbb{F}_q$ occurs exactly $q^{r-1}$ times in the set consisting of $\{a \cdot \Phi(y) \,|\, y \in \mathbb{F}_q^r\}$. Note that $h(x) \neq 0$ for all $x \in \mathbb{F}_q^s$. Therefore, for any $c \in F_q$, $f(x, y) = h(x) \cdot \Phi(y) + t(x) = c$ has $q^{s+r-1} = q^{m-1}$ solutions of $(x, y)$ in $\mathbb{F}_q^m$ where $x \in \mathbb{F}_q^s$ and $y \in \mathbb{F}_q^r$. Thus, $f(x, y)$ is balanced.

□

In the following, we set $s = 1$ and $r = m - 1$.

**Construction**:

1. Choose $u_i(x), 0 \le i < q^r - 1$, $q^r - 1$ functions from $\mathbb{F}_q$ to $\mathbb{F}_{q^r}$ which satisfy the following three conditions.
   (a) For any $x \in \mathbb{F}_q$, $u_i(x) \neq 0$, $0 \le i < q^r - 1$.
   (b) For any fixed $x \in \mathbb{F}_q$, $\{u_0(x), u_1(x), \cdots, u_{q^r-2}(x)\}$ is a permutation of $\mathbb{F}_{q^r}^*$, i.e.,
   $$\{u_0(x), u_1(x), \cdots, u_{q^r-2}(x)\} = \mathbb{F}_{q^r}^*.$$
   (c) $u_j(x)$ is not a scalar multiple of $u_i(x)$ for $i \neq j$, i.e., there is no $a \in \mathbb{F}_{q^r}$ such that $u_j(x) = au_i(x), x \in \mathbb{F}_q$ when $i \neq j$.
2. Set $\Phi(y) = y^t$ with $\gcd(t, q^r - 1) = 1$, which is a permutation of $\mathbb{F}_{q^r}$, and choose $t(x)$ any permutation of $\mathbb{F}_q$ with $t(0) \neq 0$.

In the following, we write the elements of $\mathbb{F}_{q^m}$ as a pair $(x, y)$ where $x \in \mathbb{F}_q$ and $y \in \mathbb{F}_{q^r}$ $(r = m - 1)$. We construction a set of functions from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ as follows.

$$S = \{u_i(x) \cdot \Phi(y) + at(x) \mid 0 \le i < q^r - 1, a \in \mathbb{F}_q\} \cup \{bt(x) \mid b \in \mathbb{F}_q^*\}$$

where $u_i(x) \cdot \Phi(y)$ is the dot product of $u_i(x)$ and $\Phi(y)$ when they are identified as two vectors over $\mathbb{F}_q$ of dimension $r$. If $q = 2$, then we simply use $t(x) = x$.

We may feature the above three conditions for $u_i(x)$ using the following array. Let $\mathbb{F}_q = \{\alpha_0 = 0, \alpha_1 = 1, \alpha_2, \cdots, \alpha_{q-1}\}$, and let $H = (h_{ij})$ be a $(q^r - 1) \times q$ array whose entries are given by $u_{ij} = u_i(\alpha_j), 0 \le i < q^r - 1, 0 \le j < q$, i.e.,

$$U = \begin{pmatrix} u_0(\alpha_0) & u_0(\alpha_1) & \cdots u_0(\alpha_{q-1}) \\ u_1(\alpha_0) & u_1(\alpha_1) & \cdots u_1(\alpha_{q-1}) \\ \vdots & & \\ u_{q^r-2}(\alpha_0) & u_{q^r-2}(\alpha_1) & \cdots u_{q^r-2}(\alpha_{q-1}) \end{pmatrix}$$

The three conditions on $u_i(x)$ are as follows: (a) $u_{ij} \neq 0, 0 \le i < q^r - 1, 0 \le j < q$; (b) each column of $U$ is a permutation of elements of $\mathbb{F}_{q^r}^*$; and (c) each row is not a scalar multiple of another row.

**Theorem 4.** *Let $K$ be the set consisting of sequences which are evaluations of functions in $S$. Then $K$ produces a $(N, q^m - 1, 1, d)$ LCZ signal set using the construction given in Theorem 2.*

In order to prove Theorem 4, we need the following two lemmas.

**Lemma 3.** *With the notation in Theorem 4, for $q > 2$, there exist some $a, \delta \in \mathbb{F}_q^*$ wuch that*

$$t(\delta x) = at(x), \forall x \in \mathbb{F}_q$$

*if and only if $a = 1$ and $\delta = 1$.*

*Proof.* Let $t(x) = \sum_{i=0}^{q-2} t_i x^i, t_i \in \mathbb{F}_q$ (note the fact that $t(x)$ is a permutation of $\mathbb{F}_q$ implies that $t_{q-1} = 0$). Thus

$$t(\delta x) = at(x) \Longrightarrow \sum_{i=0}^{q-2} t_i \delta^i x^i = a \sum_{i=0}^{q-2} t_i x^i. \tag{18}$$

Hence (18) is true if and only if $t_i \delta^i = at_i$ for all $i$ with $0 \leq i \leq q-2$. For those $i$'s such that $t_i \neq 0$, we have $\delta^i = a$. This yields

$$t(\delta \cdot 1) = ag(1) - at_0 + t_0. \tag{19}$$

On the other hand, we have

$$t(\delta \cdot 1) = at(1). \tag{20}$$

Substituting it into (19), we have $t_0 - at_0 = 0$. Since $t_0 \neq 0$ by the assumption, this derives that $a = 1$. Then we have $t(\delta) = t(1)$. Since $t(x)$ is a permutation, $\delta = 1$ which completes the proof.

□

**Lemma 4.** *Let $u(x)$ be a function from $\mathbb{F}_q$ to $\mathbb{F}_{q^r}$, $\Phi(y)$ be an arbitrary permutation of $\mathbb{F}_{q^r}$, and $h(x)$ be a function of $\mathbb{F}_q$. Then $u(x) \cdot \Phi(y) = h(x)$ if and only if both $u(x)$ and $h(x)$ are zero functions, i.e., $u(x) = 0$ and $h(x) = 0$.*

*Proof.* If $u(x)$ is not a zero function, then there exists some $x_0 \in \mathbb{F}_q$ such that $u(x_0) \neq 0$. Since $\Phi(y)$ is a permutation of $\mathbb{F}_{q^r}$, each element of $\mathbb{F}_q$ occurs exactly $q^{r-1}$ times in $\{u(x_0) \cdot \Phi(y) \mid y \in \mathbb{F}_{q^r}\}$. Thus this set is not equal to $\{h(x_0)\}$ which consists of only one element in $\mathbb{F}_q$.

□

*Proof of Theorem 4.* We need to show that the sequences in $K$ satisfies the following three conditions:

1. Each sequence in $K$ is balanced with period $q^m - 1$.
2. The term-by-term difference of any two of sequences in $K$ is balanced.
3. Any two sequences in $K$ are shift distinct.

Note that $t(x)$, considered as a function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, is balanced. Thus, according to Lemma 2, the condition (a) for $h_i(x)$ shows that each function in $S$ is balanced. For two functions $f(x, y)$ and $g(x, y)$ in $S$, we have the following three cases.

| | $f(x,y)$ | $g(x,y)$ |
|---|---|---|
| (i) | $u_i(x) \cdot \Phi(y) + at(x), a \in \mathbb{F}_q$ | $u_j(x) \cdot \Phi(y) + bt(x), b \in \mathbb{F}_q$ |
| (ii) | $u_i(x) \cdot \Phi(y) + at(x)$ | $bt(x)$ |
| (iii) | $at(x)$ | $bt(x)$ |

For cases (ii) and (iii), it is obvious that $f(x, y) - g(x, y)$ is balanced. For case (i), we have $f(x, y) - g(x, y) = [u_i(x) - u_j(x)] \cdot \Phi(y) + (a - b)t(x)$, according to condition (b) of the $u_i$'s, $u_i(x) - u_j(x) \neq 0$ for all $x \in \mathbb{F}_q$. Again using Lemma 2, $f(x, y) - g(x, y)$ is balanced. Thus the difference of any two functions in $S$ is balanced.

If two sequences given by $f(x, y)$ and $g(x, y)$ are shift equivalent, then we have

$$g(x, y) = f(\delta x, \sigma y), x, \delta \in \mathbb{F}_q, y, \sigma \in \mathbb{F}_{q^r}. \tag{21}$$

From Lemmas 3 and 4, if $f(x, y)$ and $g(x, y)$ belong to the cases (ii) and (iii), then they are shift distinct. So, we only need to consider case (i) for these two functions.

We use the self-dual basis in $\mathbb{F}_{q^r}$, then we can write $u_i(x) \cdot \Phi(y) = Tr_1^r(u_i(x)y^t)$ where $\Phi(y) = y^t$. Thus we have

$$f(\delta x, \sigma y) = u_i(\delta x) \cdot \Phi(\sigma y) + at(\delta x) = Tr_1^r(u_i(\delta x)\sigma^t y^t) + at(\delta x)$$
$$g(x, y) = Tr_1^r(u_j(\delta x)y^t) + bt(x)$$

$$g(x, y) = f(\delta x, \sigma y) \Longrightarrow Tr_1^r\left([u_i(\delta x)\sigma^t - u_j(x)]y^t\right) = bt(x) - at(\delta x).$$

Again using the interchange of the dot product and the trace representation, the above identity yields

$$u(x) \cdot y^t = h(x)$$

where $u(x) = u_i(\delta x)\sigma^t - u_j(x)$ and $h(x) = bt(x) - at(\delta x)$. Applying Lemma 4, we obtain that $u(x) = 0$ and $h(x) = 0$. For $h(x) = 0$, we have $bt(x) =$

$at(\delta x)$. According to Lemma 3, it follows that $a = b$ and $\delta = 1$. Substituting $\delta = 1$ into $u(x) = 0$, we have $u_j(x) = \sigma^t u_i(x)$. According to the condition (c) of the construction of $u_i(x)$'s, it follows that $i = j$ and $\sigma = 1$. Therefore $f(x, y) = g(x, y)$. Thus, any two sequences in $K$ are shift-distinct, and $|K| = (q^r - 1)q + (q - 1) = q^m - 1$.

□

From Theorems 3, the construction achieves the upper bound on the size of the LCZ signal set. We list the functions in $S$ as $S = \{g_i \mid 0 \leq i < q^m - 1\}$. Using Proposition 1, the matrix $H = (h_{i,j})$ whose entries are given by $h_{i+1,j+1} = \omega^{g_i(\alpha_j)}, 0 \leq i, j < q^m - 1$, and $h_{0,j} = 1, 0 \leq j < q^m$ and $h_{i,0} = 1, 0 \leq i < q^m$, is a Hadamard matrix in which any two row vectors in $H^-$ are shift distinct.

*Example 1.* Let $m = 4$, $q = 2$, $\mathbb{F}_{2^3}$ be defined by $\alpha^3 + \alpha + 1 = 0$ and $\mathbb{F}_{2^4}$ be defined by $\lambda^4 + \lambda + 1 = 0$. We choose $h_i(x)$, a function from $\mathbb{F}_2$ to $\mathbb{F}_{2^3}$, given as follows, which satisfy the three conditions of $h_i(x)$, $0 \leq i < 7$.

| $i$ | $u_i(0)$ | $u_i(1)$ |
|---|---|---|
| 0 | 001 | 010 |
| 1 | 010 | 011 |
| 2 | 100 | 111 |
| 3 | 011 | 001 |
| 4 | 110 | 100 |
| 5 | 111 | 110 |
| 6 | 101 | 101 |

Set $\Phi(y) = y^3$. We denote the elements of $\mathbb{F}_{2^4}$ as $\lambda_i$ and represent $\lambda^i = x_3\lambda^3 + x_2\lambda^2 + x_1\lambda + x_0, x_i \in \mathbb{F}_2$ as a pair $(x, y)$ where $x = x_3$ and $y = x_2\lambda^2 + x_1\lambda + x_0$. The set $K$ consists of fifteen binary sequences of period 15, in which the first seven sequences, denoted by $\mathbf{s}_i, i = 0, \cdots, 6$, are given by $f(x, y) = u_i(x) \cdot \Phi(y)$, which are listed in Table 1. The second group of seven sequences are given by $u_i(x) \cdot y^3 + x$ which can be obtained from $\mathbf{s}_i$ by the complement bits which correspond to $x = 1$, and the last one is given by $x$ which is $\{Tr_1^4(\lambda^i)\}_{i \geq 0}$, i.e., 000100110101111. This gives an LCZ signal set with parameters $\left(2^{4k} - 1, 15, 1, \frac{2^{4k}-1}{15}\right)$ for any positive integer $k > 1$, which achieves maximum size for these parameters.

**Table 1.** Seven sequences given by $u_i(x) \cdot \Phi(y)$

| $i$ | $\lambda^i$ $= x\lambda^3 + y$ | $y^3$ | $\mathbf{s}_0$ | $\mathbf{s}_1$ | $\mathbf{s}_2$ | $\mathbf{s}_3$ | $\mathbf{s}_4$ | $\mathbf{s}_5$ | $\mathbf{s}_6$ |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0001 | 001 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0010 | 011 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 2 | 0100 | 101 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| 3 | 1000 | 000 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0011 | 100 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| 5 | 0110 | 111 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 6 | 1100 | 101 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 7 | 1011 | 100 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| 8 | 0101 | 110 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |
| 9 | 1010 | 011 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 10 | 0111 | 010 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 11 | 1110 | 111 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| 12 | 1111 | 010 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 13 | 1101 | 110 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 14 | 1001 | 001 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |

## 4 Conclusion and Open Problems

We use two known results in the recent book by Golomb and Gong [2]:

(a) Definition of correlation for sequences over $\mathbb{F}_q$ where $q = p^t, t > 1$ (Chapter 5 in [2]); and

(b) Autocorrelation of a subfield reducible sequence over $\mathbb{F}_q$ with trace representation $f \circ h$ where $h(x)$ is a function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^m}$ with the two-tuple balance property where $m$ is a proper factor of $n$, $f(x)$ is a balanced function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ whose autocorrelation functions has the value $-1$ everywhere except for $\tau = jd, j = 0, 1, \cdots, q^m - 2$ where $d = \frac{q^n-1}{q^m-1} = q^{m(l-1)} + q^{m(l-2)} + \cdots q^m + 1$ (where $n = lm$), and for $\tau = jd$, the autocorrelation of the sequence at $jd$ is equal to the autocorrelation of the sequence given by $f$ at $j, j = 0, 1, \cdots$. (Theorem 8.2 and Corollary 8.3 in [2].)

Consequently, we obtain a huge set of subfield reducible sequences over $\mathbb{F}_q$ of period $q^n - 1$ with correlation values $-1$ everywhere except for the values at $\tau = jd, 0 \leq j < q^m - 1$ where $m$ is a proper factor of $n$. The number of sequences in this set is equal to the number of balanced functions from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ divided by $q^m - 1$. From this result, we constructed the signal set $\Pi_0$ with low correlation zone, i.e., the crosscorrelation of any two sequences or autocorrelation of any sequence in this set is equal to $-1$ for the absolute value of $\tau \neq 0$ and less than $d$. The size of $\Pi_0$ is equal to the number of shift-distinct balanced sequences over $\mathbb{F}_q$ with period $q^m - 1$. From $\Pi_0$, we derived the other two signal sets with the same parameters as those of $\Pi_0$, but one consists of sequences over $\mathbb{Z}_q$ and the other consists of sequences over the complex $q$-th roots of unity where $q = p^t$ for $t > 1$.

If we require the crosscorrelation of any two sequences in $\Pi_0$ is equal to $-1$ at $\tau = 0$, we showed that from the subfield factorization construction, the size of any LCZ signal set cannot exceed $q^m - 1$, the relationship between these functions and Hadamard matrices, and we also provided a construction for this type of signal set in which the size achieves the maximum for any $q$.

For research on finding some new constructions of subfield reducible sequences over $\mathbb{F}_q$ with 2-level autocorrelation, or with low correlation and/or with low correlation zone, it would be worthwhile to put some effort into the following unsolved problems.

**Construction of $h(x)$ in the set $\Pi_0$:**

Any sequence in $\Pi_0$ is given by $f \circ h(x)$ where $f(x) : \mathbb{F}_{q^m} \to \mathbb{F}_q$ with the balanced property and $h(x) : \mathbb{F}_{q^n} \to \mathbb{F}_{q^m}$ with either (a) the two-tuple balance property, or (b) with $k$-form and the difference balance property. The other construction for $h(x)$ using $f \circ h(x)$ produces a sequence with an interleaved structure (see [2] for details).

There are only two known constructions for $h(x)$ being either two-tuple balanced or being $k$-form with the difference balance property.

(i) $h(x)$ is a single trace term, i.e., $h(x) = Tr_m^n(x^k)$, which gives $m$-sequences over $\mathbb{F}_q$.

(ii) $h(x)$ is a cascaded GMW function of length $s$, which produces a cascaded GMW sequence over $\mathbb{F}_q$.

Up to now, neither two-tuple balanced functions nor $k$-form functions with the difference balance property have been found which do not fall into one of the above two cases.

Open Question 1: Is the converse of Fact 1 true? In other words, is the two-tuple balance property on a function $h(x) : \mathbb{F}_{q^n} \to \mathbb{F}_{q^m}$ equivalent to the condition of both $k$-form and the difference balance property of the function $h(x)$?

Open Question 2: For each such $h(x)$, we have a set $\Pi_0$, which is an almost low correlation zone signal set with parameters $(q^n - 1, r, 1, d)$ where $r$ is the number of shift-distinct balanced sequences over $\mathbb{F}_q$ with period $q^m - 1$, and $d = \frac{q^n-1}{q^m-1}$. Thus the most interesting realizations for $\Pi_0$ are those in which the evaluations of the $h(x)$'s are neither $m$-sequences nor (cascaded) GMW sequences. In other words, does there exist a function $h(x) : \mathbb{F}_{q^n} \to \mathbb{F}_{q^m}$ whose evaluation is neither an $m$-sequence nor a (cascaded) GMW sequence but which has the two-tuple balance property (or, sufficiently, which is $k$-form with the difference balance property)?

## References

1. R. De. Gaudenzi, C. Elia, and R. Viola, Bandlimited quasisynchronous CDMA: A novel satellite access technique for mobile and personal communication systems, *IEEE J. Select. Area Commun.*, vol. 10, pp. 328-343, Feb. 1992.

2. S. W. Golomb and G. Gong, *Signal Designs with Good Correlation: for wireless communications, cryptography and radar applications*, Cambridge University Press, 2005.
3. G. Gong and S. W. Golomb, The decimation-Hadamard transform of two-level autocorrelation sequences, *IEEE Trans. Inform. Theory*, vol. 48, pp. 853-865, 2002.
4. G. Gong and H.-Y. Song, Two-tuple balance of non-binary sequences with ideal two-level autocorrelation, abstract in the *Proceedings of 2003 IEEE International Symposium on Information Theory*, June 29 - July 4, Yokohama, Japan, pp.404, full version as Technical Report CORR 2002-20, Center for Advanced Cryptographic Research, University of Waterloo, 2002.
5. S.-H. Kim, J.-W. Jang, J.-S. No, and H. Chung, New constructions of quaternary low correlation zone sequences, *IEEE Trans. Inform. Theory*, vol. 51, no. 4, pp. 1469-1477, April 2005.
6. A. Klapper, $d$-form sequences: a family of sequences with low correlation values and large linear spans, *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 423-431, March 1995.
7. A. Klapper, A. H. Chan, and M. Goresky, Cross-correlations of linearly and quadratically related geometric sequences and GMW sequences, *Discrete Appl. Math.*, vol. 46, no. 1, pp. 1-20, 1993.
8. B. Long, P. Zhang, and J. Hu, A generalized QS-CDMA system and the design of new spreading codes, *IEEE Trans. Veh. Tech.*, vol. 47, pp. 1268-1275, Nov. 1998.
9. X. H. Tang and P. Z. Fan, A class of pseudonoise sequences over GF($p$) with low correlation zone, *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1644-1649, May 2001.