[5] M. Y. Rosenbloom and M. A. Tsfasman, "Codes for the m-metric," *Probl. Inf. Transm.*, vol. 33, no. 1, pp. 45–52, 1997.
[6] P. O. Vontobel and A. Ganesan, An Explicit Construction of Universally Decodable Matrices, 2005, Tech. Rep. [Online]. Available: http://www.arxiv.org/abs/cs.IT/0508098.
[7] P. O. Vontobel and A. Ganesan, "On universally decodable matrices for space-time coding," *Des. Codes Cryptogr.*, vol. 41, pp. 325–342, Dec. 2006.
[8] H. Hasse, "Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik," *J. Reine. Ang. Math.*, vol. 175, pp. 50–54, 1936.
[9] R. R. Nielsen, "A class of Sudan-decodable codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1564–1572, Jul. 2000.

A Note on Low-Correlation Zone Signal Sets

Guang Gong, *Member, IEEE*, Solomon W. Golomb, *Fellow, IEEE*, and Hong-Yeop Song, *Senior Member, IEEE*

***Abstract*—In this correspondence, 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. This results in LCZ 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 qth root of unity. We show a connection between these sequence designs and "completely noncyclic" Hadamard matrices and a construction for those sequences. We also provide some open problems along this direction.**

***Index Terms*—Hadamard matrices of completely noncyclic type, low-correlation zone (LCZ) sequences, subfield reducible sequences, two-tuple balance property.**

I. Introduction

Recently, there have been some interesting developments involving quasi-synchronous (QS) code-division multiple-access (CDMA) communication systems and on the design of sequences with low-correlation zone (LCZ) that can be used in such systems [2], [12], [13], [8], [11], [14].

This correspondence will describe a general approach to the design of LCZ sequences using the results on sequences with subfield decompositions, presented in [3, Ch. 8] written by the first two authors. The above known cited results on LCZ sequences can be obtained easily from this general setting.

The connection between an optimal set of LCZ sequences (in terms of family size) with subfield factorization and Hadamard matrices have been observed now by many others, e.g., see [14]. We show, in particular, that the LCZ sequences in this correspondence are connected to Hadamard matrices of "completely noncyclic type."

Manuscript received February 25, 2006; revised September 14, 2006. The work of H.-Y. Song was supported by the Basic Research Program of the Korea Science & Engineering Foundation under Grant (R01-2003-000-10330-0). The material in this correspondence was presented in part at the 2006 Conference of Information Sciences and Systems, Princeton University, Princeton, NJ, March 2006.

G. Gong is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: ggong@calliope.uwaterloo.ca).

S. W. Golomb is with the Department of Electrical Engineering—Systems, University of Southern California, Los Angeles, CA 90089 USA (e-mail: milly@usc.edu).

H.-Y. Song is with the School of Electrical and Electronics Engineering, Yonsei University, Seoul 120-749, Korea (e-mail: hysong@yonsei.ac.kr).

Communicated by A. Canteaut, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2007.899538

Notation

We use the following notation throughout the correspondence.

- 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.
- α always denotes a primitive element of $\mathbb{F}_{q^n}$.
- Let $\mathbf{a} = \{a_i\}$ be a sequence over $\mathbb{F}_q$ of period $q^n - 1$. Using the (discrete) Fourier transform, there exists a polynomial function $f(x)$ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ such that $a_i = f(\alpha^i), i = 0, 1, \ldots$, 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 α, or $\mathbf{a}$ is an evaluation of $f(x)$ (for details, see [3]). For any function $f(x)$ appearing in this correspondence, 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 $f(\mathbf{x}) = f(x_1, \ldots, x_n)$ where $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$. 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 $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. 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 $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ and $\mathbf{x} \cdot \mathbf{y} = \sum_i^n x_i y_i$, the dot product of $\mathbf{x}$ and $\mathbf{y}$.
- A function $f(x)$ with $f(0) = 0$ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is balanced if each element in $\mathbb{F}_q$ occurs in $\{f(x)|x \in \mathbb{F}_{q^n}\}$ exactly q^{n-1} times. Let $\{a_i\}$ be a sequence over $\mathbb{F}_q$ of period $q^n - 1$, and $g(x)$ be its trace representation. Then, we say $\{a_i\}$ is balanced if $g(x) - g(0)$ is balanced.
- Two periodic sequences $\{a_i\}$ and $\{b_i\}$ over $\mathbb{F}_q$ of period P are said to be shift-equivalent if there exists some integer k $(0 \leq k < P)$ such that $b_i = a_{i+k}$ for all i. Otherwise, they are called shift-distinct.

A. *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 [3], and we will use the following (see Question 16 in Exercises for [3, Ch. 5]).

Let η be a primitive qth root of unity, i.e., there is some integer j such that $\eta = \exp(\frac{ij2\pi}{q})$ where $i = \sqrt{-1}$. Let $\{\beta_0, \beta_1, \ldots, \beta_{t-1}\}$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. For $x \in \mathbb{F}_q$, we have

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

We define

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

0018-9448/$25.00 © 2007 IEEE

which is a p-ary representation of an integer x in Z_q. Then ρ gives 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, for $\tau = 0, 1, \ldots$

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

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

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

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

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

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

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

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

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

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

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

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

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 correspondence for sequences over $\mathbb{F}_q$ are valid for the other two classes of sequences.

In the rest of the correspondence, for simplicity, we will omit the map ρ in correlation calculation, but it should be understood that if $q = p^t, t > 1$, x in $\eta^x, x \in \mathbb{F}_q$ represents the p-ary 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.

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

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 (9), in fact, is the definition of the crosscorrelation between two functions $a(x)$ and $b(x)$ [3]. In other words, the crosscorrelation between $a(x)$ and $b(x)$, denoted by $C_{a,b}(\lambda)$, is defined as

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

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

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

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

B. LCZ and Almost LCZ Sequences

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

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

then S is referred to as an (N, r, δ, d) low correlation zone (LCZ) signal set. For the CDMA communication systems working in the quasisynchronous mode, it is well-known that the crosscorrelation function of spreading codes around the origin determines the performance [12]. If the crosscorrelation of any two sequences in S satisfies the following conditions:

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

we call S an (N, r, δ, d) almost low correlation zone (ALCZ) signal set. It is an LCZ signal set except possibly for the higher crosscorrelation value exactly at the origin, i.e., at $\tau = 0$.

According to this definition, if $d = \lceil N/2 \rceil$, then a (N, r, δ, d) LCZ signal set becomes a (N, r, δ) 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 [12], [13], [8], [11], [14].

It is quite interesting to observe that all such LCZ signal sets come from a well-known fact which is presented in [3]. In the following two sections, we present this relation and a construction that achieves the upper bound on the size of the signal set. In the final section, we give a few open problems and some concluding remarks.

II. Crosscorrelation of Subfield Reducible Sequences

Definition 1: (Golomb and Gong, 2005 [3, Definition 8.3]) Let $f(x)$ be a function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ with $f(0) = 0$ and let

$$\Omega_f(\lambda) = \{(f(x), f(\lambda x)) \,|\, x \in \mathbb{F}_{q^n}^*\}, 1 \neq \lambda \in \mathbb{F}_{q^n}^*. \quad (14)$$

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 $(0,0) \neq (\theta, \mu) \in \mathbb{F}_q^2$ occurs q^{n-2} times in $\Omega_f(\lambda)$ and $(0,0)$ occurs $q^{n-2} - 1$ times in $\Omega_f(\lambda)$.

2) For $1 \neq \lambda \in \mathbb{F}_q^*$, there exists some $1 \neq \mu \in \mathbb{F}_q^*$ such that $(0,0) \neq (\theta, \mu\theta)$ occurs q^{n-1} times in $\Omega_f(\lambda)$ for every $\theta \in \mathbb{F}_q^*$ and $(0,0)$ occurs $q^{n-1} - 1$ times in $\Omega_f(\lambda)$.

Definition 2: (Gong and Golomb, 2002 [4]) 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

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

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 [3], 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 $\tau \not\equiv 0 \pmod d$ and the autocorrelation of $a(x)$ for $\tau \equiv 0 \pmod d$ is equal to the autocorrelation of $f(x)$ multiplied by a scalar factor. (Refer to [3, Theorem 8.1 and Corollary 8.2] for details.) They also illustrated the effect of autocorrelation of this type of subfield reducible sequences using an example (in [3, Example 8.2]). In other words, there are only $q^m - 1$ autocorrelation values at τ's which are multiples of d which are undetermined. Compared to those τ's whose correlation values are equal to -1 (there are $q^n - q^m$ such τ's), the number of undetermined values is relatively quite small and these τ 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 [10] and k-form sequences [9] 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 (see [10]) and the proof also can be given in a similar fashion to that for their autocorrelation functions. Unfortunately, these results have not received sufficient publicity. We reproduce it here.

Recall that $Q = q^m$, and $n = lm$, and let $d = \frac{q^n-1}{q^m-1}$.

Theorem 1: Let h be a function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_Q$ with the two-tuple balance property, and f and g be any two functions from $\mathbb{F}_Q$ to $\mathbb{F}_q$. Let $\mathbf{a}$ and $\mathbf{b}$ be two sequences, not necessarily distinct, 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

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

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

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

Proof: Note first that $\lambda \neq 0$. For $\lambda \neq 1$,

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

Assume $\lambda \notin \mathbb{F}_Q$. In this case, substituting Condition 1 of Definition 1 into (16), we have

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

Now, assume $0 \neq \lambda \in \mathbb{F}_Q$. Substituting Condition 2 of Definition 1 into (16), we have, since $1 \neq \mu \in \mathbb{F}_Q^*$

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

For $\lambda \in \mathbb{F}_Q^*$, since $\beta = \alpha^d$ is a primitive element in $\mathbb{F}_Q$, we may write $\lambda = \beta^j = \alpha^{jd} \implies \tau = jd$ 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, their cross-correlation function takes the value -1 for all τ's which are not multiples of d; i.e., there are $q^n - q^m$ values of τ 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 τ remaining at which the cross-correlation value is undetermined. These undetermined values depend on the cross correlation between f and g, i.e., $C_{f\circ h, g\circ h}(\alpha^{id}) = q^{n-m} C_{f,g}(\beta^i)$, $i = 0, 1, \ldots, q^m - 2$, where $\beta = \alpha^d$.

Observe that the condition that makes $C_{f\circ h, g\circ h}(\lambda) = 0$ for so many values of τ 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, which map zero to zero. Then the sequential 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 Π_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 we have the following.

1) Any two sequences in Π_0 are shift-distinct.
2) For any two sequences in Π_0, say $\mathbf{a}$ and $\mathbf{b}$

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

Moreover, Π_0 is a $(N, r, 1, d)$ almost LCZ signal set where $|\Pi_0| = r = |U^-|$.

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 [3, Sec. 8.1]). 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.

Remark 1: The size r of Π_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 $f(\mathbf{x}) = cx_1 + f_1(x_2, \ldots, x_m), c \in \mathbb{F}_q^*$, is a balanced function where $f_1(x_2, \ldots, x_m)$ 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).

Remark 2: For $q = p^t$ where $t > 1$, let Π_1 and Π_2 be the sets consisting of the sequences over $\mathbb{Z}_q$ transformed from Π_0 by (4) and the sequences over the complex field transformed from Π_0 by (6), respectively. Then both Π_1 and Π_2 are $(N, r, 1, d)$ almost LCZ signal sets.

Remark 3: A function $h(x) : \mathbb{F}_{q^n} \to \mathbb{F}_{q^m}$ is k-form, if, for any $\lambda \in \mathbb{F}_{q^m}^*$ and $x \in \mathbb{F}_{q^n}$, $h(\lambda x) = \lambda^k h(x)$, $\gcd(k, q^n - 1) = 1$. A function $h(x) : \mathbb{F}_{q^n} \to \mathbb{F}_{q^m}$ has the difference balance property, if, for any $\lambda \in \mathbb{F}_{q^n}, \lambda \neq 1$, $h(x) - h(\lambda x)$ is balanced. In 2002 [6], Gong and Song established essentially *Fact 1* given below. The known results on LCZ sequences come from the general construction for Π_0, in which either h is a monomial trace term [12], [13] for $q = 2$ or $q = p$, or $h(x)$ satisfies both k-form and the difference balance property [8] for $q = 2^2$. In all these 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 also can be easily established via exponential sums together with *Fact 1*. *Fact 1* also implies that, if $h(x)$ is k-form and difference balance property, then it has the two-tuple balance property.

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.

Note that if $C_{f \circ h, g \circ h}(0) = 0$ or equivalently $C_{f,g}(0) = 0$, then Π_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. We now concentrate on the subset K of U^- in the following section.

III. A Construction of K

In this section, we provide an important observation on the achievable upper bound for the size of K, a set of balanced sequences in which the term-by-term difference of any two distinct members is also balanced. For this, we give a connection between the existence of K and the Hadamard matrices as a fact in the following, whose proof can be easily established by some elementary method in linear algebra. We also give a construction for K whose size achieves this upper bound.

Let $\{a_i\}$ be a sequence over $\mathbb{F}_q$ of period P. We say that $\{a_i\}$ is balanced if

$$|N_x - N_y| \leq 1, \quad \text{for any } x, \ y \in \mathbb{F}_q$$

where

$$N_x = |\{i | a_i = x, 0 \leq i < P\}|, \quad x \in \mathbb{F}_q.$$

Note that this definition is a general case of the balance property defined earlier for $P = q^n - 1$.

Fact 2: 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.

When the period is $q^m - 1$, note that the above implies that the size $|K|$ of K is upper bounded by $q^m - 1$.

In this following, we show the relation of the set K and a q-ary Hadamard matrix. Recall that q is a power of a prime.

Let $H = (h_{ij})_{v \times v}$ where $h_{ij} = \omega^{s_{ij}}, s_{ij} \in \mathbb{F}_q$ and ω is a primitive qth root of unity. Here, the map in (2) should be used when $q = p^t$ for a prime p and $t > 1$. H is said to be a *Hadamard matrix* if $HH^* = vI_v$ where $H^* = (h_{ij}^*)$ where x^* is the complex conjugate of x and I_v is the $v \times v$ identity matrix. In other words, H is a Hadamard matrix if the Hermitian inner product of any two row vectors of H is equal to zero, i.e., any two row vectors of H are orthogonal.

Note that H can always be transformed into a special form in which the first row and the first column are the all one's vectors by applying some elementary "Hadamard-preserving" operations [1], [3]. Therefore, without loss of generality, we may assume that H is in this form. 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.

Theorem 3: Use the notations above. Let $H = (h_{ij})$ 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 ω is a primitive element of $\mathbb{F}_q$. Let K be a set consisting of the sequences whose trace representations are g_j's, $1 \leq j < q^m$. Then K produces an LCZ signal set with parameters $(N, r_0, 1, d)$ if and only if H is a Hadamard matrix. Furthermore, in such a case, $r_0 = q^m - 1$ if and only if any two rows of H^- are shift distinct when they are considered as sequences. Here, H^- is the reduced form in size $(q^m - 1) \times (q^m - 1)$ assuming H is in the form in which the first row and the first column are the all one's vectors.

Therefore, the classification of all the LCZ signal sets with parameters $(N, q^m - 1, 1, d)$ constructed by the subfield decomposition (Theorem 2) is equivalent to the classification of all the $q^m \times q^m$ Hadamard matrices in which the row vectors in the reduced forms are all shift distinct. We may call this a Hadamard matrix of a completely noncyclic (or super noncyclic) type. For these K's, the size of K achieves the maximum possible value (Fact 2).

Note that for the known constructions, $|K| < q^{m-1}$ for $q = p$ [13], $|K| = q^{m/2}$ for $q = 2^2$ [8]. While this manuscript was in preparation, two more results were presented at some conferences [11], [14]. In these results, the size of the set K was attained to be $q^m - 1$ where $q = p$, and the relation of K and a completely noncyclic type Hadamard matrix was observed. These are the results that again proves Theorem 1.

In the following, we give another construction for K in which the size $|K|$ 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. So, we will directly proceed it for a general q, a power of a prime (which is either 2 or an odd prime p).

A Construction for K:

STEP 1: We write the elements of $\mathbb{F}_{q^m}$ as a pair (x, y) where $x \in \mathbb{F}_q$ and $y \in \mathbb{F}_{q^r}$ where we set $r = m - 1$.

STEP 2: Choose $u_i(x), 0 \leq i < q^r - 1, q^r - 1$ functions from $\mathbb{F}_q$ to $\mathbb{F}_{q^r}$ which satisfy the following three conditions.

(a) For any $x \in \mathbb{F}_q$, $u_i(x) \neq 0, 0 \leq i < q^r - 1$.

(b) For any fixed $x \in \mathbb{F}_q$, $\{u_0(x), u_1(x), \ldots, u_{q^r-2}(x)\}$ is a permutation of $\mathbb{F}_{q^r}^*$, i.e.,

$$\{u_0(x), u_1(x), \ldots, u_{q^r-2}(x)\} = \mathbb{F}_{q^r}^*.$$

(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 $i \neq j$.

STEP 3: Set $\Phi(y) = y^v$ with $\gcd(v, q^r - 1) = 1$, which is a permutation of $\mathbb{F}_{q^r}$, and choose $t(x)$ any permutation of $\mathbb{F}_q$ with $t(0) \neq 0$ for $q > 2$, and choose $t(x) = x$ for $q = 2$.

STEP 4: Construct a set of functions from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ as follows.

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

We now let K be the set consisting of sequences which are evaluations of functions in S.

Theorem 4: Let K be the set constructed according to the steps described above. Then K produces a $(N, q^m - 1, 1, d)$ LCZ signal set using the construction given in Theorem 2.

We may feature the above three conditions for $u_i(x)$ using the following array. Let $\mathbb{F}_q = \{\alpha_0 = 0, \alpha_1 = 1, \alpha_2, \ldots, \alpha_{q-1}\}$, 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.

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

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.

For the proof of Theorem 4, we need a series of lemmas.

Lemma 2: We write the elements of $\mathbb{F}_{q^m}$ as a pair (x, y) where $x \in \mathbb{F}_q^s$ and $y \in \mathbb{F}_{q^r}$ where $m = r + s$. Let $h(x)$ 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 $\mathbb{F}_q^r$, 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 $\mathbb{F}_q$, where $h(x) \cdot \Phi(y)$ is the dot product of r-tuple vectors.

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 $\{a \cdot \Phi(y) \mid y \in \mathbb{F}_q^r\}$. 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. □

Lemma 3: With the notation in Theorem 4, for $q > 2$, there exist some $a, \delta \in \mathbb{F}_q^*$ such 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 $t_i \delta^i = a t_i$ for all i with $0 \le i \le q-2$. For those i's such that $t_i \neq 0$, we have $\delta^i = a$. This yields

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

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 $u(x) \cdot \Phi(y) = h(x)$ for all $x \in \mathbb{F}_q$ and $y \in \mathbb{F}_{q^r}$ if and only if both $u(x)$ and $h(x)$ are zero functions, i.e., $u(x) = 0$ and $h(x) = 0$ for all $x \in \mathbb{F}_q$.

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 $t(x)$ is a permutation of $\mathbb{F}_q$, and hence, is balanced. Thus, according to Lemma 2, the condition (a) for $u_i(x)$ 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 to consider:

	$f(x,y)$	$g(x,y)$
(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 $u_i(x) \cdot \Phi(y) = Tr_1^r(u_i(x)y^v)$ where $\Phi(y) = y^v$. Thus, we have

$$\begin{aligned} f(\delta x, \sigma y) &= u_i(\delta x) \cdot \Phi(\sigma y) + at(\delta x) \\ &= Tr_1^r(u_i(\delta x)\sigma^v y^v) + at(\delta x) \\ g(x,y) &= Tr_1^r(u_j(\delta x) y^v) + bt(x). \end{aligned}$$

Hence, $g(x,y) = f(\delta x, \sigma y)$ implies $Tr_1^r([u_i(\delta x)\sigma^v - u_j(x)]y^v) = bt(x) - at(\delta x)$. Again using the interchange of the dot product and the trace representation, the above identity yields

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

where $u(x) = u_i(\delta x)\sigma^v - u_j(x)$ 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 $u_j(x) = \sigma^v u_i(x)$. 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 and 4, we have the following.

Corollary 1: The construction for K above also constructs a completely noncyclic Hadamard matrix over $\mathbb{F}_q$ of size $q^m \times q^m$. Total number $M(q,m)$ of such Hadamard matrices from the above construction is given by

$$M(q,m) \geq \frac{\prod_{i=0}^{q-1}[(q^r-1)!-(q^i-1)]}{q!}\phi(q^r-1)[q!-(q-1)!]$$

where $r = m-1$ and $\phi(n)$ is the Eulor's-ϕ-function that counts the number of integers from 1 to n which are relatively prime to n.

Proof: For each $u_i(x)$ there are $(q^r-1)!$ choices for an image. The lower bound is obtained by taking out all the nontrivial linear combinations of the $u_j(x)$'s, $j = 0,1,\ldots,i-1$, when $u_i(x)$ is to be selected for each $i = 0,1,\ldots,q-1$. □

From Theorem 2, 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 Theorem 4, 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 completely noncyclic Hadamard matrix, i.e., 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 $u_i(x)$, a function from $\mathbb{F}_2$ to $\mathbb{F}_{2^3}$, given as follows, which satisfy the three conditions of $u_i(x), 0 \leq i < 7$.

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 λ_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 $\mathbf{s}_i, i = 0,\ldots,6$, are given by $f(x,y) = u_i(x)\cdot\Phi(y)$, which are listed in Table I. 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 $k > 1$. The resulting 16×16 Hadamard matrix of completely noncyclic type is shown in Fig. 1. Note that the reduced form of size 15×15 without the first row and first column is completely noncyclic.

TABLE I
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

$$\left[\begin{array}{c|ccccccccccccccc}
+ & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + \\
\hline
+ & - & - & - & + & + & - & + & + & + & - & + & - & - & - & + \\
+ & + & - & + & + & + & - & - & + & - & + & - & + & - & - & - \\
+ & + & + & - & + & - & - & + & - & - & + & + & - & - & + & - \\
+ & - & + & - & + & + & + & - & + & - & - & - & - & + & + & - \\
+ & + & - & - & + & - & + & - & - & + & + & - & - & + & - & + \\
+ & - & + & + & + & - & - & - & - & + & - & - & + & - & + & + \\
+ & - & - & + & + & - & + & + & - & - & - & + & + & + & - & - \\
\hline
+ & - & - & - & - & + & - & - & - & + & + & + & + & + & + & - \\
+ & + & - & + & - & + & - & + & - & - & - & - & - & + & + & + \\
+ & + & + & - & - & - & - & - & + & - & - & + & + & + & - & + \\
+ & - & + & - & - & + & + & + & - & - & + & - & + & - & - & + \\
+ & + & - & - & - & - & + & + & + & + & - & - & + & - & + & - \\
+ & - & + & + & - & - & - & + & + & + & + & - & - & + & - & - \\
+ & - & - & + & - & - & + & - & + & - & + & + & - & - & + & + \\
\hline
+ & + & + & + & - & + & + & - & - & + & - & + & - & - & - & -
\end{array}\right]$$

Fig. 1. A 16 by 16 Hadamard matrix whose reduced form of size 15 by 15 is completely noncyclic. See Example 1.

IV. CONCLUSION AND OPEN PROBLEMS

We use two known results in the recent book by Golomb and Gong [3]:

a) Definition of correlation for sequences over $\mathbb{F}_q$ where $q = p^t, t > 1$ ([3, Ch. 5]); 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 $\tau = jd, j = 0,1,\ldots,q^m-2$ 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 $j, j = 0,1,\ldots$ (see [3, Theorem 8.2 and Corollary 8.3]).

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 Π_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 Π_0 is equal to the number of shift-distinct balanced sequences over $\mathbb{F}_q$ with period $q^m - 1$. From Π_0, we derived the other two signal sets with the same parameters as those of Π_0, but one consists of sequences over $\mathbb{Z}_q$ and the other consists of sequences over the complex qth roots of unity where $q = p^t$ for $t > 1$.

If we require the crosscorrelation of any two sequences in Π_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 sets 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 two-level autocorrelation, or with low correlation and/or with LCZ, it would be worthwhile to put some effort into the following unsolved problems.

Construction of $h(x)$ in the Set Π_0: Any sequence in Π_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 [3] 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 for q which is a power of 2.

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 $\mathbb{F}_q$.

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 $h(x)$ for q which is a power of any prime?

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, i) and ii), for q which is a power of 2.

Open Question 2: For each such $h(x)$, we have a set Π_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 Π_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) for q which is equal to 2 or a power of 2? For q a power of an odd prime, Kim *et al.* showed (see [7, Theorem 5]) that the HG functions are 1-form with the difference-balance property. This is another type of $h(x)$ with this property, in addition to i) and ii) mentioned above.

Open Question 3: From Theorems 3 and 4, we found that the set K of maximum size is in the one-to-one correspondence with a Hadamard matrix in which any two rows are shift-distinct. These Hadamard matrices are not just "noncyclic" type since no two rows in the reduced form are shift-equivalent. We may call this type "super noncyclic" or "completely noncyclic." Classification of all the completely noncyclic type Hadamard matrices would be an interesting future work.

REFERENCES

[1] R. Craigen, "Hadamard matrices and designs," in *CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds. New York: CRC, 1996, ch. IV.24, pp. 370–377.

[2] 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, pp. 328–343, Feb. 1992.

[3] S. W. Golomb and G. Gong, *Signal Designs With Good Correlation: For Wireless Communications, Cryptography and Radar Applications*. Cambridge, U.K.: Cambridge University Press, 2005.

[4] G. Gong and S. W. Golomb, "The decimation-Hadamard transform of two-level autocorrelation sequences," *IEEE Trans. Inf. Theory*, vol. 48, pp. 853–865, 2002.

[5] G. Gong, S. W. Golomb, and H.-Y. Song, "A Note on Low Correlation Zone Signal Sets," Technical Report University of Waterloo, Center of Advanced Cryptographic Research, Canada, CORR 2006-03, 2006.

[6] G. Gong and H.-Y. Song, "Two-tuple balance of nonbinary sequences with ideal two-level autocorrelation," in *Proc. 2003 IEEE Int. Symp. Inf. Theory*, Yokohama, Japan, Jun.–Jul. 29–4, 2003, p. 404.

[7] S.-H. Kim, J.-S. No, H. Chung, and T. Helleseth, "New cyclic relative difference sets constructed from d-homogeneous functions with difference-balanced property," *IEEE Trans. Inf. Theory*, vol. 51, pp. 1155–1163, Mar. 2005.

[8] 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.

[9] A. Klapper, "d-form sequences: A family of sequences with low correlation values and large linear spans," *IEEE Trans. Inf. Theory*, vol. 41, pp. 423–431, Mar. 1995.

[10] A. Klapper, A. H. Chan, and M. Goresky, "Cross-correlations of linearly and quadratically related geometric sequences and GMW sequences," *Discr. Appl. Math.*, vol. 46, no. 1, pp. 1–20, 1993.

[11] J.-W. Jang, J. S. Chung, J.-S. No, and H. Chung, "New sets of optimal p-ary low correlation zone sequences," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, Jul. 10–14, 2006.

[12] B. Long, P. Zhang, and J. Hu, "A generalized QS-CDMA system and the design of new spreading codes," *IEEE Trans. Veh. Technol.*, vol. 47, pp. 1268–1275, Nov. 1998.

[13] X. H. Tang and P. Z. Fan, "A class of pseudonoise sequences over $\mathrm{GF}(p)$ with low correlation zone," *IEEE Trans. Inf. Theory*, vol. 47, pp. 1644–1649, May 2001.

[14] X. H. Tang and P. Udaya, "New recursive construction of low correlation zone sequences," in *Proc. Second Int. Workshop Sequence Design and Its Applicat. Commun.*, Shimonoseki, Japan, Oct. 10–14, 2005.

A New Family of Ternary Almost Perfect Nonlinear Mappings

Geir Jarle Ness and Tor Helleseth, *Fellow, IEEE*

***Abstract*—A mapping $f(x)$ from $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p^n)$ is differentially k-uniform if k is the maximum number of solutions $x \in \mathrm{GF}(p^n)$ of $f(x+a) - f(x) = b$, where $a, b \in \mathrm{GF}(p^n)$ and $a \neq 0$. A 2-uniform mapping is called almost perfect nonlinear (APN). This correspondence describes new families of ternary APN mappings over $\mathrm{GF}(3^n)$, $n \geq 3$ odd, of the form $f(x) = ux^{d_1} + x^{d_2}$ where $d_1 = \frac{3^n-1}{2} - 1$ and $d_2 = 3^n - 2$.**

***Index Terms*—Almost perfect nonlinear (APN), ternary mappings.**

I. INTRODUCTION

Let $\mathrm{GF}(p^n)$ be the finite field with p^n elements and let $\mathrm{GF}(p^n)^*$ denote the set of nonzero elements in the field. Let $f(x)$ be a mapping $f : \mathrm{GF}(p^n) \to \mathrm{GF}(p^n)$. Let $N(a,b)$ denote the number of solutions $x \in \mathrm{GF}(p^n)$ of $f(x+a) - f(x) = b$ where $a, b \in \mathrm{GF}(p^n)$ and let

$$\Delta_f = max\{N(a,b) \mid a, b \in \mathrm{GF}(p^n), a \neq 0\}.$$

The value Δ_f is called the *differential uniformity* of the mapping f. A mapping is said to be differentially $k-$ uniform if $\Delta_f = k$. This is of interest in cryptography since differential and linear cryptanalysis exploit weaknesses of the uniformity of functions of the form $f(x) = x^d$ over $\mathrm{GF}(p^n)$ where p is a prime. For applications in cryptography one would like to find functions where Δ_f is small. When $p = 2$, the solutions come in pairs, therefore, $\Delta_f = 2$ is the smallest possible value. When $\Delta_f = 2$, we call the functions almost perfect nonlinear

Manuscript received October 30, 2006; revised March 27, 2007. This work was supported by the Norwegian Research Council.

The authors are with the Selmer Center, Department of Informatics, University of Bergen, PB 7803, N-5020 Bergen, Norway (e-mail: geirn@ii.uib.no; tor.helleseth@ii.uib.no).

Communicated by A. Canteaut, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2007.899508