Low Correlation Zone Signal Sets

Guang Gong

Department of Electrical & Computer Engineering
University of Waterloo
CANADA

Joint work with Solomon W. Golomb and Hong-Yeop Song

University of Waterloo

Outline of Presentation

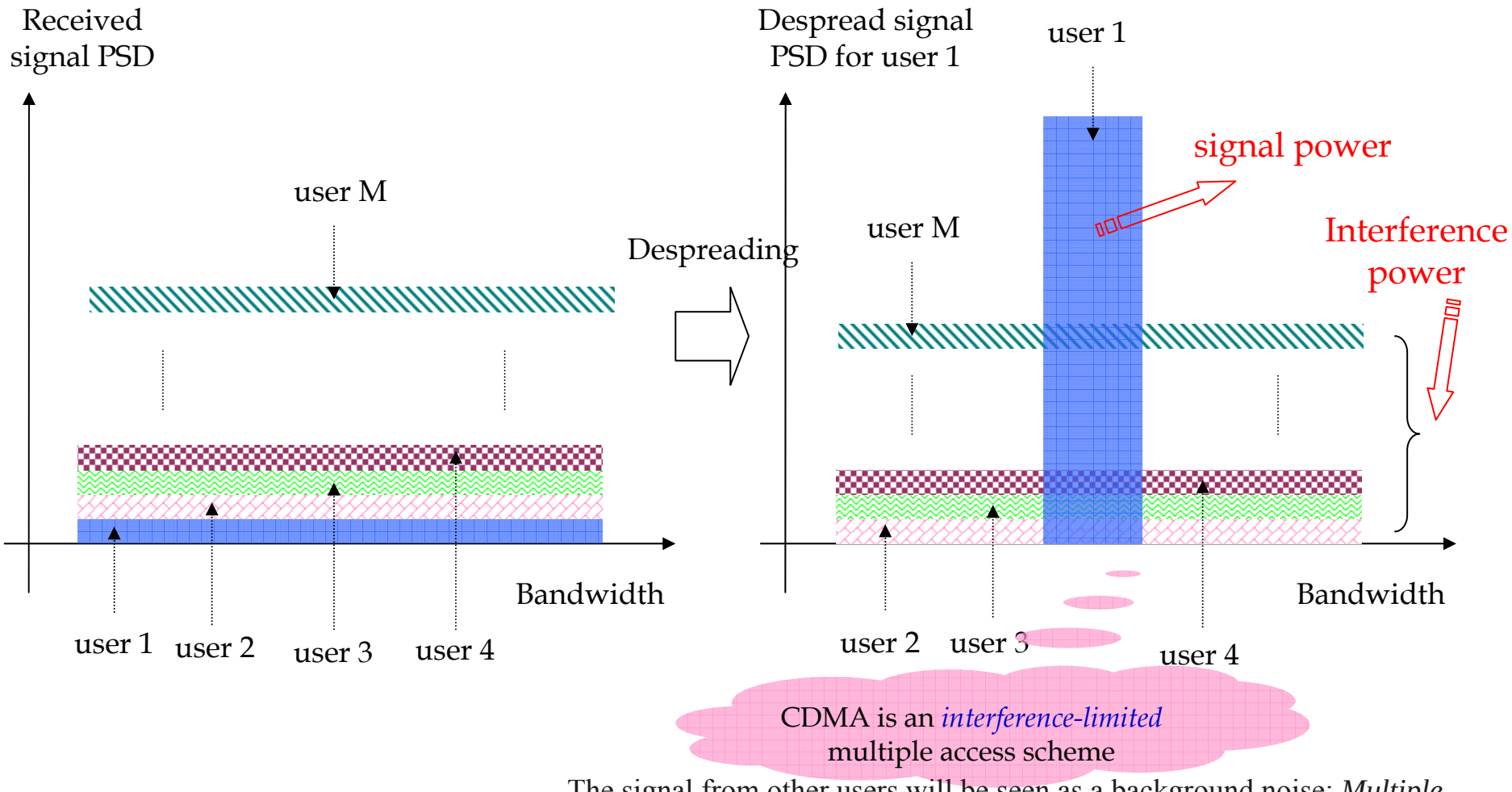
- Requirements of Spreading Sequences in Quasi-synchronous (QS) CDMA Communications
- Definitions of Three Types Correlations, LCZ and Almost Signal Sets
- Correlation of Subfield Reducible Sequences
- Relationship between Subfield Constructions of LCZ Sequences and Complete Non-Cycle Hadamard Matrixes
- A New Construction of Subfield LCZ Sequences
- Open Questions

Code Division Multiplexing Access (CDMA)

- Multiple users share a common channel simultaneously by using different *codes*
- Narrowband user information is spread into a much wider spectrum by the spreading code
- The signal from other users will be seen as a background noise: Multiple access interference (MAI)
- The limit of the maximum number of users in the system is determined by interference due to multiple access and multipath fading: Adding one user to CDMA system will only cause graceful degradation of quality

Theoretically, no fixed maximum number of users !

Code Division Multiplexing Access (CDMA) (Cont.)



The signal from other users will be seen as a background noise: *Multiple access interference (MAI)*

Spreading Sequences in CDMA Systems

$H_n \times H_n^T = nI_n$

Walsh Codes: Basic spreading codes in CDMA systems

- *n* different Walsh codes: each row of an *nxn* Hadamard matrix
- Mutually orthogonal: inner product of different Walsh codes are zero
- Synchronization of all users are required to maintain the orthogonality: Otherwise, produce multiple access interference (MAI)
- Further, delayed copies received from a multipath fading are not orthogonal any more: Multipath fading interference

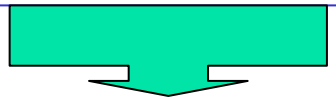
MAI and multipath interference are major factors to limit the capacity of CDMA systems !

Quasi-synchronous CDMA Systems

- Synchronous CDMA
  - Strict synchronization is required
  - Spreading codes having perfect orthogonality at zero time delay are ideal
  - Concern: What if multipath fading introduces nonzero time delay that can destroy the orthogonality of orthogonal codes?

- Asynchronous CDMA
  - No synchronization between transmitted spreading sequences is required
  - Relative delays between spreading sequences are arbitrary
  - Nonzero interference due to multiple users and multipath fading is not avoidable: Interference cancellation or Multiuser detection process is required

- Quasi-synchronous CDMA
  - Approximately synchronous CDMA (AS-CDMA)
  - Originally proposed for satellite communications (1992)
  - It may be feasible to maintain a chip or a few chips synchronization especially in microcell or indoor environment
  - Relative time delay of a few chips is allowed
  - *Synchronized system with some synchronization errors*



Sequence design criterion: within a few chips, correlation between different spreading codes should be as low as possible

Three Types of Correlations

- Notations: p a prime, $q = p^t$, $N = q^n - 1$ $\mathbf{a} = \{a_i\}$, $\mathbf{b} = \{b_i\}$ two sequence over F_q

Let η be a primitive qth 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

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

We define

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

Three Types of Correlations (Cont.)

(Golomb and Gong, 2005)

The crosscorrelation between a and b is defined as, for $\tau = 0, 1, \cdots,$

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

Three Types of Correlations (Cont.)

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.

Three Types of Correlations (Cont.)

An unaware fact about correlation of these three different alphabet sets:

$$C_{\mathbf{a,b}}(\tau) = C_{\mathbf{u,v}}(\tau) = C_{\mathbf{s,t}}(\tau)$$

LCZ and Almost LCZ Sequences

Let $\mathrm{s}_j = (s_{j,0}, s_{j,1}, \cdots, s_{j,N-1}), 0 \le j < r$, be r shift-distinct sequences over $\mathbb{F}_q$ with period N. Let $S = \{\mathrm{s}_0, \mathrm{s}_1, \cdots, \mathrm{s}_{r-1}\}$. If for any two sequences in S, say a and b, $C_{\mathrm{a,b}}(\tau)$, the correlation function between a and b defined by (3), satisfies $|C_{\mathrm{a,b}}(\tau)| \le \delta$, 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 a and b in S, we have

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

where $\tau \neq 0$ for **a** = **b**. Then S is referred to as a (N, r, δ, d) low correlation zone (LCZ) signal set.

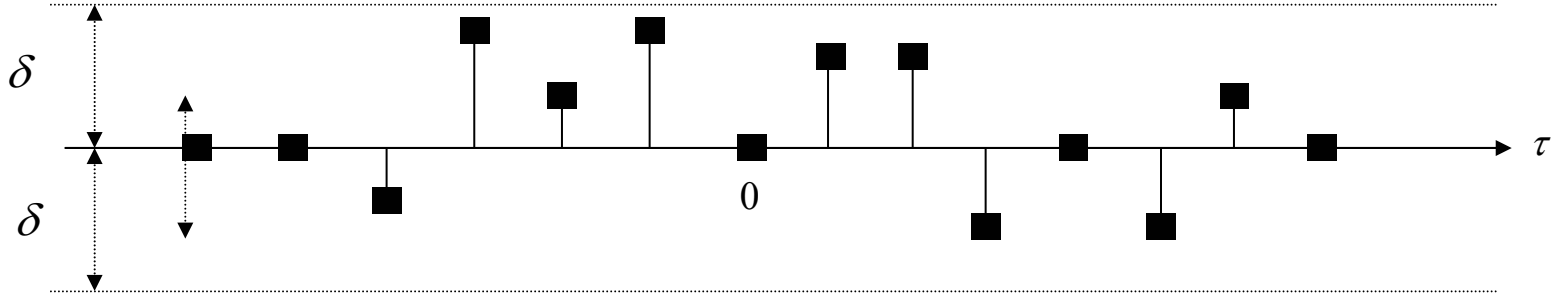
If the crosscorrelation/out-of-phase autocorrelation of any two sequences a and b in S satisfies

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

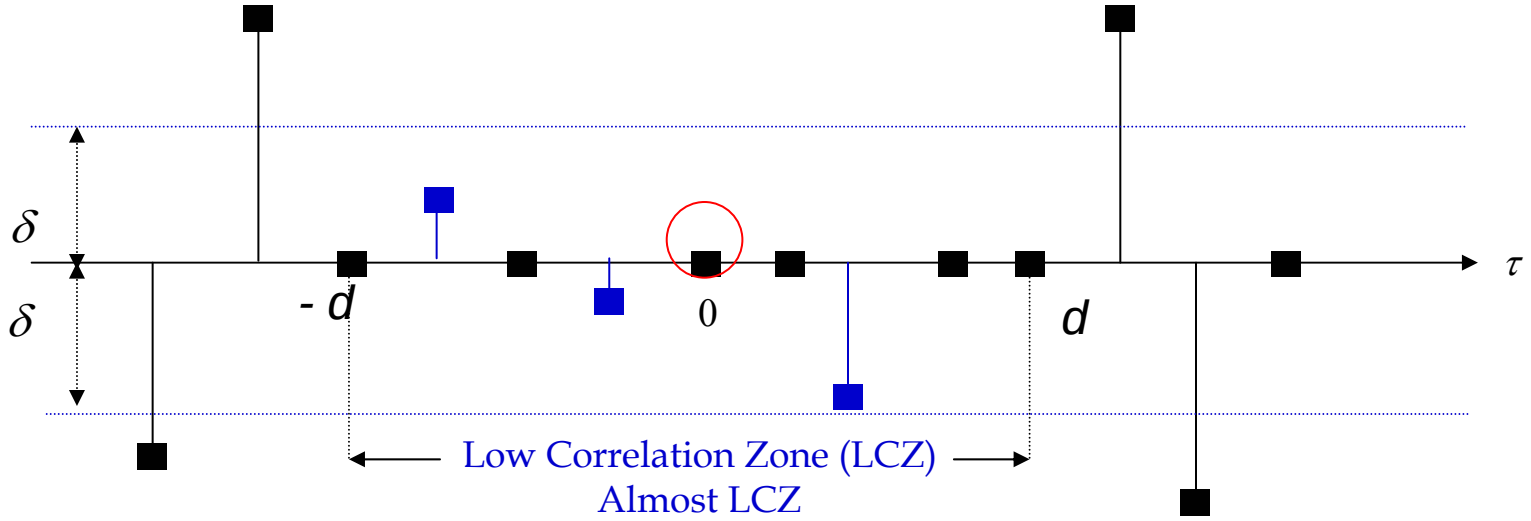
Then S is called a (N, r, δ, d) almost LCZ signal set.

LCZ and Almost LCZ Sequences (Cont.)

Conventional low correlation



(Almost) Low correlation zone



Crossorrelation of Subfield Reducible Sequences

From now on, we will also use trace representations of sequences over F_q with period N.

Definition 2 (Gong and Golomb, 2002 [3] Def. 8.4) *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

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

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.

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*

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

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

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

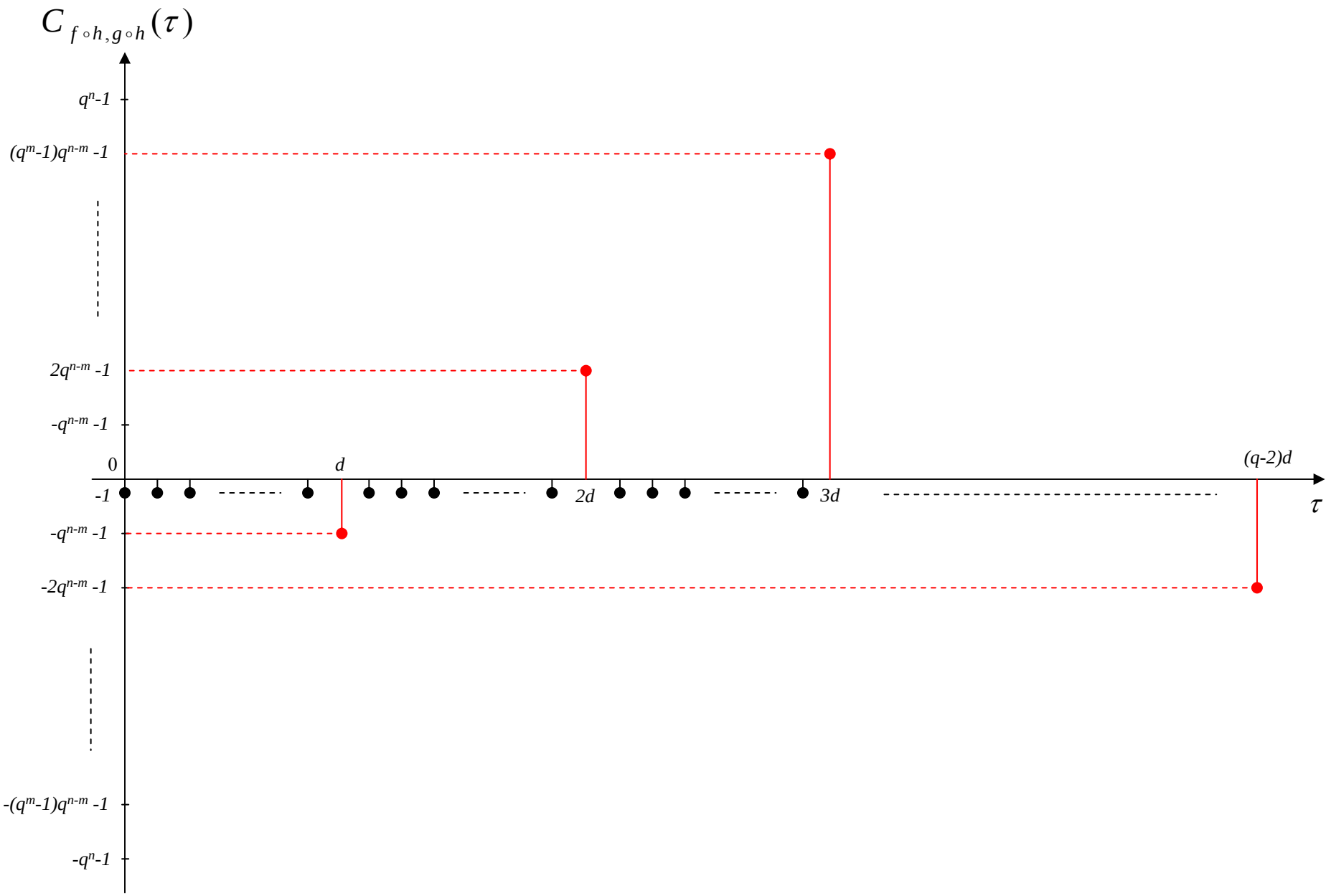
where $d = \dfrac{q^n - 1}{q^m - 1}$

Remarks on Theorem 1

1) Known binary cases (Klapper, Chan and Goresky (1993), and Klapper (1995)) :

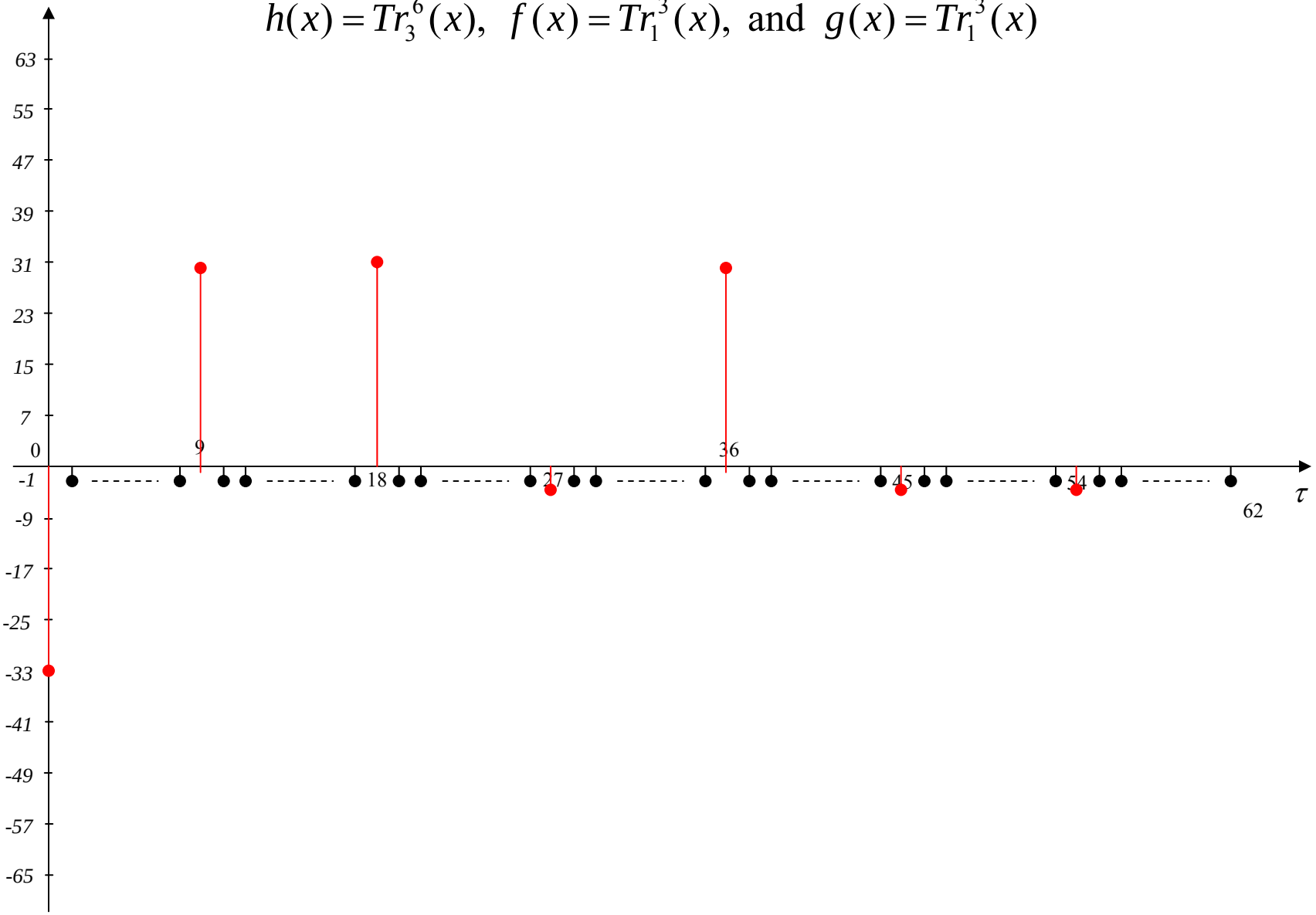
- $h(x)$ is a trace monomial function or a cascaded GMW function
- $h(x)$ is a k-form function

2) If both of f and g are balanced, then crosscorrelation/out-of-phase autocorrelation between f and g takes value of -1 for $q^n - q^m$ shifts, and the only at most $q^m - 1$ correlation values may be irregular.


$C_{f\circ h, g\circ h}(\tau)$
q^n-1
$(q^m$-1)q^{n-m} -1
$2q^{n-m}$ -1
$-q^{n-m}$ -1
0
-1
d
2d
3d
(q-2)d
τ
$-q^{n-m}$ -1
$-2q^{n-m}$ -1
$-(q^m$-1)q^{n-m} -1
$-q^n$-1

$C_{f\circ h, g\circ h}(\tau)$

$$h(x) = Tr_3^6(x),\ \ f(x) = Tr_1^3(x),\ \text{and}\ \ g(x) = Tr_1^3(x)$$



Relationship between Subfield Constructions of LCZ Sequences and Complete Non-Cycle Hadamard Matrixes

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 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*

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 $|\Pi_0| = r = |U^-|$.

Subfield Constructions of LCZ Seq. and Complete Non-Cycle Hadamard Matrixes (Cont.)

Corollary 1 *Recall that U^- denotes a set consisting of all the shift-distinct balanced sequences over $\mathbf{F}_q$ of period q^m-1, and let $K \subset U^-$ in which the term-by-term difference of two distinct sequences is also balanced. Then the size $|K|$ of K is upper bounded by q^m-1.*

For the known constructions: $|K| < p^m - 1$ for $q = p$ (Tang-Fan, 2001); $|K| = q^{m/2}$ for q = 2^2 (Kim etc. 2005); $|K| = 2^m - 1$ for $q = 2$ or p (Jang etc. 2005; Tang and Udaya, 2005, Jang etc. 2006).

Subfield Constructions of LCZ Seq. and Complete Non-Cycle Hadamard Matrixes (Cont.)

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. 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 inner (or Hermitian dot if $q > 2$) product of any two row vectors of H is equal to zero, i.e., any two row vectors of H are orthogonal.

Theorem 4 *Use the notations above. Let $H = (h_{ij})$ be a $q^m \times q^m$ matrix over $\mathbf{F}_q$, and let $g_j(\alpha^i) = s_{ij}$ where $h_{ij} = \omega^{s_{ij}}, s_{ij} \in \mathbb{F}_q$ and α 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 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.*

Subfield Constructions of LCZ Sequences and Complete Non-Cycle Hadamard Matrixes (Cont.)

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 call this type of Hadamard matrix a completely non-cyclic (or super non-cyclic). For these K's, the size of K achieves the maximum possible

An LCZ signal set with parameters $(N, q^m - 1, 1, d)$ ⟺ A complete non-cyclic Hadamard matrix,

Classification of subfield reducible LCZ signal sets with the above parameters ⟺ Classification of $q^m \times q^m$ complete non-cyclic Hadamard matrices

A New Construction of Subfield LCZ Sequences

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 $u_i(x), 0 \le i < q^r - 1$, $q^r - 1$ 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 $i \neq j$.

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 $q = 2$.

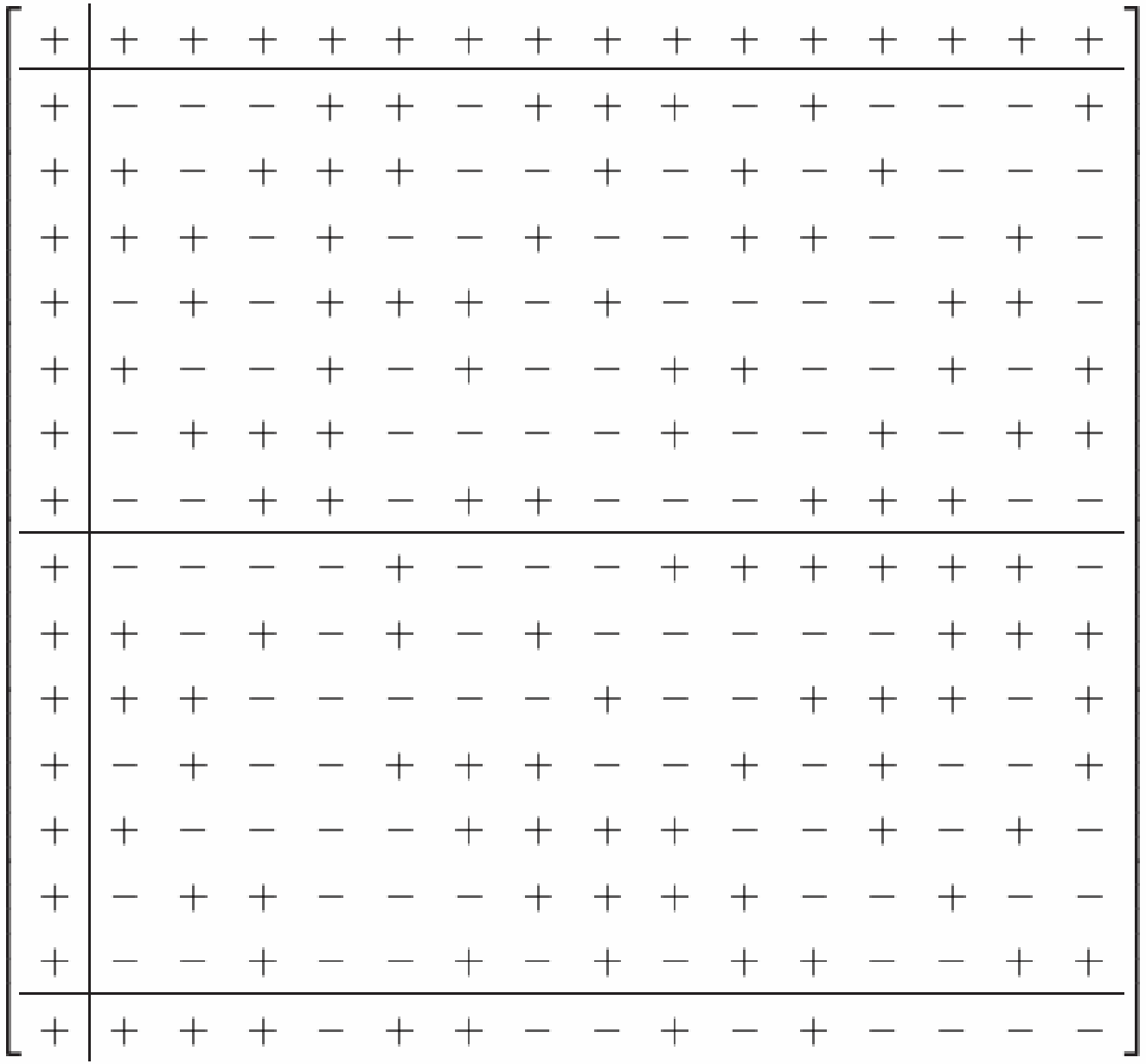
STEP 4 Construct a set of functions from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ as follows.

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

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

Then K produces a subfield reducible LCZ signal sets for any q with parameters

$$(N, q^m - 1, 1, d)$$



Open Problems for Characteristic 2 Case

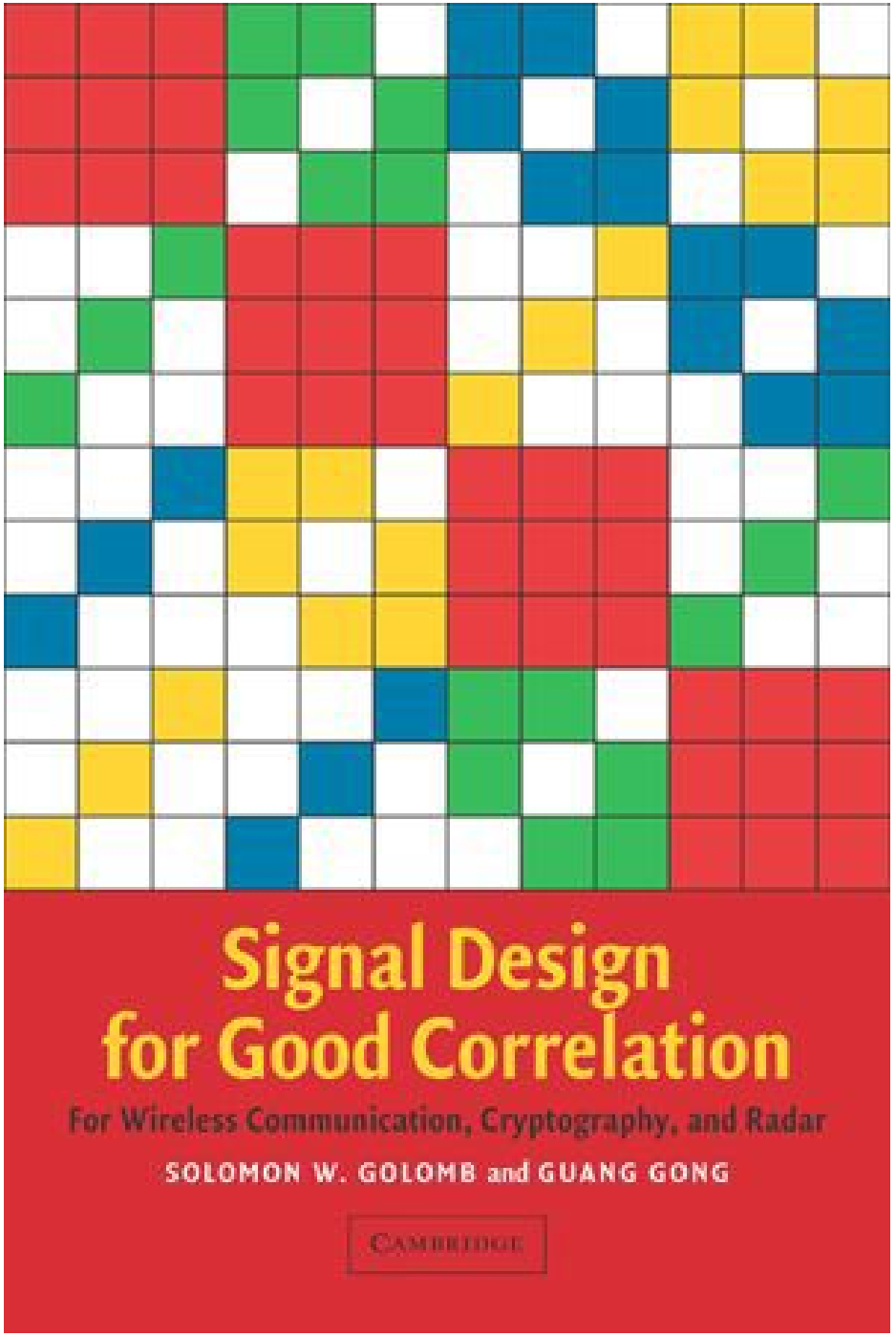
Open Question 1. Is that true that $h(x)$, $F_{q^n} \to F_{q^m}$ with 2-tuple-balance property is equivalent to that $h(x)$ is k-form with difference balance property. Recall that $h(x)$ is k-form if and only if

$$h(yx) = y^k h(x), \quad y \in F_{q^m}, \quad x \in F_{q^m}$$

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 $h(x) : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^m}$ 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)?

Open Question 3: From Theorems 4 and 5, we found that the set K of maximum size is in one to one correspondence with Hadamard matrix in which any two rows are shift-distinct. These Hadamard matrices are not just "non-cyclic" type since no two rows in the reduced form are shift-equivalent. We may call this type "super non-cyclic" or "completely non-cyclic." Classification of all the completely non-cyclic type Hadamard matrices would be an interesting future work.

For more about correlation of subfield reducible sequences, see Golomb and Gong's new book:



Reference

Guang Gong, Solomon W. Golomb, and Hong-Yeop Song,

A Note on Low Correlation Zone Signal Sets,

- *Proceedings of 40th Annual Conference of Information Sciences and Systems* (CISS 2006), March 22-24, 2006, Princeton University.

- Technical Report, University of Waterloo, CACR 2006-06, January 2006.