Correlation of Multiple Bent Function Signal Sets

Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
Email. ggong@calliope.uwaterloo.ca

Abstract

Observing a phenomenon that the pre-image set of nonzero Hadamard spectra of the composition of a function and a trace function is independent of the function, a construction of multiple bent function signal sets using different bent functions is given. Their correlation and high-order shift-distinct property are discussed. As a by-product, the union of the multiple bent function signal sets produces a signal set with low correlation zone and much larger size of the other known constructions.

Index Terms. Multiple signal sets, maximum correlation, bent functions, high-order shift-distinct property, CDMA.

1 Introduction

Pseudorandom sequences with good correlation have wide applications in communications and cryptography. Communications over networking environments bring up many new problems in sequence design. For example, interference in detect of code division multiple access (CDMA) signals is not only from signals within one signal set, but also from several different signal sets when users roam to different geographical areas. (For detection of CDMA signals, the reader is referred to [20][19][18].) This type of interference is referred to as *intraference* among these signal sets in the engineering content, i.e., correlation among multiple signal sets. In this paper, we consider correlation and high-order shift-distinct property of multiple signal sets constructed from bent function signal sets.

2 The Basic Definitions and Properties

A *crosscorrelation function* between two binary sequences $\mathbf{a} = \{a_i\}$ and $\mathbf{b} = \{b_i\}$ with period N is defined by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{N-1} (-1)^{a_{i+\tau}+b_i}, \tau = 0, 1, \cdots$$

When $\mathbf{a} = \mathbf{b}$, the crosscorrelation between $\mathbf{a}$ and $\mathbf{b}$ becomes the autocorrelation of $\mathbf{a}$.

The shift operator is defined by $L\mathbf{a} = a_1, a_2, \cdots$ for $\mathbf{a} = a_0, a_1, \cdots$, and $L^r\mathbf{a} = a_r, a_{r+1}, \cdots$. For two sequences, if one can be obtained from the other by performing the shift operator, then we say that they are *shift equivalent*. Otherwise, they are said to be *shift distinct*. Let S be a set consisting of r shift-distinct binary sequences of period N. The maximum correlation of S is defined by

$$\delta = \max\{|C_{\mathbf{a},\mathbf{b}}(\tau)| \,|\, \mathbf{a}, \mathbf{b} \in S, |\tau| < N, \text{ and } \tau \neq 0 \text{ if } \mathbf{a} = \mathbf{b}\}.$$

S is called an (N, r, δ) *signal set*, and S is called an (N, r, δ, d) *low correlation zone signal set* if $|\tau| \leq d$ where $d < N$. (For signal sets with low correlation, see [12].)

The author introduced the following concepts about high-order shift-distinct property and correlation of multiple signal sets in [7] and discussed the multiple signal sets constructed using Kasami (or generalized Kasami) signal sets in [5].

Definition 1 *Let $S_1, \cdots, S_k$ be k signal sets with period N. They are said to be* mth-order shift distinct *if any sequence in these signal sets is not a linear combination of shifts of $m-1$ different sequences, each taken from $m-1$ different signal sets. In other words, for $\mathbf{a} \in S_i, 1 \leq i \leq k$,*

$$\mathbf{a} \neq c_1 L^{\tau_1}\mathbf{b}_{r_1} + \cdots + c_{m-1}L^{\tau_{m-1}}\mathbf{b}_{r_{m-1}}$$

for any $c_j \in \mathbb{F}_2$, $\tau_j \in \mathbb{Z}_N$, and $\mathbf{b}_{r_j} \in S_{r_j}$ with $r_j \neq i$, $j = 1, \cdots, m-1$.

If any two of $S_1, \cdots, S_k$ are shift distinct, i.e., $m = 2$, then we also say that they are *pairwise shift distinct*. In general, the pairwise shift-distinct property of multiple signal sets is easier to obtain than that of the mth-order shift-distinct property for $m > 2$. The high-order shift-distinct property also directly connects with the high-order correlation of sequences [15].

Definition 2 *Let k multiple signal sets $S_1, \cdots, S_k$, each with parameters (N, r, δ), be mth-order ($m \geq 2$) shift distinct. The maximum correlation of k multiple signal sets $S_1, \cdots, S_k$ is defined by*

$$\Delta = \max\{|C_{\mathbf{a},\mathbf{b}}(\tau)| \,|\, \mathbf{a} \in S_i, \mathbf{b} \in S_j, 1 \leq i, j \leq k, |\tau| < N\}$$

where $\tau \neq 0$ if $\mathbf{a} = \mathbf{b}$. $S_1, \cdots, S_k$ are said to be (v, r, k, Δ) multiple signal sets. *If $|\tau| \leq d$ where $d < N$, then $S_1, \cdots, S_k$ are called (v, r, k, Δ, d)* multiple low correlation zone signal sets.

Let $q = 2^n$, and α be a primitive element of $\mathbb{F}_q$. A function $f(x)$ from $\mathbb{F}_q$ to $\mathbb{F}_2$ is bent if its Hadamard transform has constant magnitude, i.e.,

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{F}_q} (-1)^{Tr(\lambda x) + f(x)} = \pm\sqrt{q}, \ \forall \lambda \in \mathbb{F}_q. \tag{1}$$

Parseval Formula: The Parseval formula states that the correlation of two sequences is equal to the correlation of their Hadamard transforms up to a scalar factor of $1/q$. In other words, let $g(x)$ be another function from $\mathbb{F}_q$ to $\mathbb{F}_2$. Then we have

$$C_{\mathbf{a},\mathbf{b}}(\tau)+1=\sum_{x\in\mathbb{F}_q}(-1)^{f(\delta x)}(-1)^{g(x)}=\frac{1}{q}\sum_{y\in\mathbb{F}_q}\widehat{f}(\delta y)\widehat{g}(y)$$

where $\mathbf{a}=\{a_i\}$ with $a_i=f(\alpha^i)$, $\mathbf{b}=\{b_i\}$ with $b_i=g(\alpha^i)$, and $\delta=\alpha^\tau$.

This paper is organized as follows. We show that the pre-image set of non-zero Hadamard spectra of a composition of a function from $\mathbb{F}_q$ from $\mathbb{F}_2$ and a trace function from $\mathbb{F}_{q^l}$ to $\mathbb{F}_q$ is independent of the composited function in Section 3. From this observation, we give a construction of multiple bent function signal sets with three valued correlations except for one shift in Section 4. Section 5 discusses the mth-order shift-distinct property of multiple bent function signal sets.

3 Pre-image Sets of Nonzero Hadamard Spectra of Composed Functions

Let $N=ln$, $Tr_n^N(x)$ denote the trace function from $\mathbb{F}_{q^l}$ to $\mathbb{F}_q$, and $g(x)$ be a function from $\mathbb{F}_q$ ($q=2^n$) to $\mathbb{F}_2$. Let

$$f(x)=g\circ Tr_n^N(x)=g(Tr_n^N(x)) \tag{2}$$

where $\circ$ is the composition operator.

Fact 1 *With the above notation,*

$$\widehat{f}(\lambda)=\begin{cases}0, & \lambda\notin\mathbb{F}_q\\ q^{l-1}\widehat{g}(\lambda), & \lambda\in\mathbb{F}_q.\end{cases}$$

In particular, if $g(x)$ is a bent function from $\mathbb{F}_q$ to $\mathbb{F}_2$, then

$$\widehat{f}(\lambda)=\begin{cases}0, & \lambda\notin\mathbb{F}_q\\ \pm q^{l-1}\sqrt{q}, & \lambda\in\mathbb{F}_q.\end{cases}$$

The validity of the above result can be derived from the results on geometrical sequences discussed by Klapper, Chan and Goresky in [10]. It can also be obtained using the following result about m-sequences generated by $Tr_n^N(x)$ (the proof can be found in [4] or the original paper [23]).

Property 1 *For $\lambda\in\mathbb{F}_{q^l}$, let*

$$P=\{(Tr_n^N(\lambda x),Tr_n^N(x))\,|\,x\in\mathbb{F}_{q^l}\}.$$

If $\lambda \notin \mathbb{F}_q$, then each pair $(\theta, \mu) \in \mathbb{F}_q \times \mathbb{F}_q$ occurs q^{l-2} times in P. If $\lambda \in \mathbb{F}_q$, then $(\lambda\mu, \mu)$ occurs q^{l-1} times in P for each $\mu \in \mathbb{F}_q$.

This is referred to as the *2-tuple balance property* of m-sequences over $\mathbb{F}_q$ in [4]. In the following, we will assume that g is a bent function from $\mathbb{F}_q$ to $\mathbb{F}_2$. Let

$$h(x) = g \circ Tr_n^{nl}(x) + Tr_1^{nl}(\beta x), \beta \in \mathbb{F}_{q^l} \setminus \mathbb{F}_q, \tag{3}$$

and $T(h) = \{y \in \mathbb{F}_{q^l} \,|\, \widehat{h}(y) \neq 0\}$, which is the pre-image set of the non-zero Hadamard spectra of h. We will show that $T(h)$ is independent of the bent function g.

Theorem 1 *With above notation, then $h(x)$ is balanced, and*

$$T(h) = \{t + \beta \,|\, t \in \mathbb{F}_q\}$$

which is independent of g.

Proof. Recall that $f(x) = g \circ Tr_n^{nl}(x)$ from (3). Then

$$\sum_{x \in \mathbb{F}_{q^l}} (-1)^{h(x)} = (-1)^{f(x)+Tr_1^N(x)} = \widehat{f}(\beta) = 0$$

where the last identity is from $\beta \notin \mathbb{F}_q$ and Fact 1. Thus h is balanced. Again using Fact 1, $\widehat{h}(y) \neq 0$ if and only if $y + \beta \in \mathbb{F}_q$. Thus $T(h)$ can be rewritten as follows.

$$T(h) = \{y \,|\, y + \beta \in \mathbb{F}_q\} = \{t + \beta \,|\, t \in \mathbb{F}_q\}$$

where $t = y + \beta$. Hence $T(h)$ is independent of the bent function g.

□

Note. This is not an intuitive phenomenon. The pre-image set of the non-zero Hadamard spectra of h is solely determined by β where g has no effect on this set.

4 A Construction of Multiple Bent Function Signal Sets

We are now ready to give a construction for multiple bent function signal sets.

Construction of Multiple Bent Function Signal Sets: Let $f_j(x) : \mathbb{F}_q \to \mathbb{F}_2$, $0 \leq j < q-1$ be shift-distinct bent functions (i.e., their corresponding sequences are shift distinct), and let ω be a primitive element of $\mathbb{F}_q$. We choose $\sigma_0 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ which is a root of some irreducible polynomial over $\mathbb{F}_q$ of form $x^2 + x + w, w \in \mathbb{F}_q$. Let

$$\begin{aligned} f_{\lambda,\omega^j}(x) &= f_j(Tr_n^{2n}(x)) + Tr_1^{2n}((\lambda + \omega^j\sigma_0)x), \\ &\quad \lambda \in \mathbb{F}_q, \omega^j \in \mathbb{F}_q^*, 0 \leq j < q-1. \end{aligned} \tag{4}$$

From now on, we write $\mu = \omega^j$. Define

$$s_{\lambda,\mu,i} = f_{\lambda,\mu}(\alpha^i), i = 0, 1, \cdots$$

where α is a primitive element of $\mathbb{F}_{q^2}$. Thus $f_{\lambda,\mu}(x)$ is the trace representation of the sequence $\mathbf{s}_{\lambda,\mu} = \{s_{\lambda,\mu,i}\}_{i\geq 0}$. Let

$$S_i = \{\mathbf{s}_{\lambda,\omega^i} \mid \lambda \in \mathbb{F}_q\}.$$

Then we have $(q-1)$ signal sets: $\{S_i \,|\, 0 \leq i < q-1\}$. For each fixed i, S_i is the original bent function signal set with parameters $(q^2-1, q, q+1)$ because $\beta^i\sigma_0 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Bent function signal sets were constructed by Olsen, Scholtz and Welch in 1982 [16].

Theorem 2 *Let $\mathbf{a} \in S_i$ and $\mathbf{b} \in S_j$ have the trace representations $f_{\eta,\theta}(x)$ and $f_{\lambda,\mu}(x)$, respectively, defined by (4) where $\theta = \omega^i$ and $\mu = \omega^j$. Then $C_{\mathbf{a},\mathbf{b}}(\tau)$, crosscorrelation between $\mathbf{a}$ and $\mathbf{b}$, is given by*

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \begin{cases} -1 \pm q & \text{if } \alpha^\tau \notin \mathbb{F}_q \\ -1 & \text{if } \alpha^\tau \in \mathbb{F}_q, \alpha^\tau \neq \theta^{-1}\mu \\ -1 + q\widehat{h}(\lambda+\eta) & \text{if } \alpha^\tau = \theta^{-1}\mu \end{cases}$$

where $h(x) = f_j(x) + f_i(\alpha^\tau x)$.

Proof. Let $\delta = \alpha^\tau$. If $\tau = 0$, then we have

$$f_{\lambda,\mu}(x) + f_{\eta,\theta}(x) = Tr_1^N(\beta x)$$

where $\beta = \lambda + \mu\sigma_0 + \eta + \theta\sigma_0$. If $\mathbf{a} \neq \mathbf{b}$, then $C_{\mathbf{a},\mathbf{b}}(0) = -1$ if and only if $\beta \neq 0$. Since $\{1, \sigma_0\}$ is basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, $\beta = 0$ if and only if $\lambda = \eta$ and $\mu = \theta$. Thus $\beta \neq 0$ if and only if $\mathbf{a} \neq \mathbf{b}$. Therefore, we have $C_{\mathbf{a},\mathbf{b}}(0) = -1$ for $\mathbf{a} \neq \mathbf{b}$. In the following, we assume that $\tau \neq 0$.

Case 1. $\delta \notin \mathbb{F}_q$. Using the Parseval formula, we have

$$\begin{aligned} C_{\mathbf{a},\mathbf{b}}(\tau) + 1 &= \sum_{x\in\mathbb{F}_{q^2}} (-1)^{f_{\lambda,\mu}(x)}(-1)^{f_{\eta,\theta}(\delta x)} \\ &= \frac{1}{q^2}\sum_{y\in\mathbb{F}_{q^2}} \widehat{f}_{\lambda,\mu}(y)\widehat{f}_{\eta,\theta}(\delta y). \end{aligned} \tag{5}$$

According to Fact 1,

$$\widehat{f}_{\lambda,\mu}(y), \widehat{f}_{\eta,\theta}(\delta y) \in \{0, \pm q\sqrt{q}\}.$$

Substituting it into (5), we obtain

$$C_{\mathbf{a},\mathbf{b}}(\tau) + 1 = \frac{1}{q^2} f_{\lambda,\mu}(y)\widehat{f}_{\eta,\theta}(\delta y) \cdot |V| = \pm q|V| \tag{6}$$

where

$$V = \{y \in \mathbb{F}_{q^2} \,|\, \widehat{f}_{\lambda,\mu}(y) \neq 0 \text{ and } \widehat{f}_{\eta,\theta}(\delta y) \neq 0\}.$$

Thus, we only need to show that either $|V| = 0$ or $|V| = 1$. Let

$$T_{s,v} = \{y \in \mathbb{F}_{q^2} \,|\, \widehat{f}_{s,v}(y) \neq 0\}, s \in \mathbb{F}_q, v \in \mathbb{F}_q^*. \tag{7}$$

Applying Theorem 1, we may write

$$T_{\lambda,\mu} = \{t + \sigma \,|\, t \in \mathbb{F}_q\}, \text{ and } T_{\eta,\theta} = \{t' + \sigma' \,|\, t' \in \mathbb{F}_q\},$$

where $t = y + \sigma$ with $\sigma = \lambda + \mu\sigma_0$ and $t' = y + \sigma'$ with $\sigma' = \eta + \theta\sigma_0$. Using this representation, we have

$$\delta^{-1}T_{\eta,\theta} = \{\delta^{-1}y \,|\, \widehat{f}_{\eta,\theta}(y) \neq 0\} = \{u \,|\, \widehat{f}_{\eta,\theta}(\delta u) \neq 0\}.$$

Thus V is the intersection of $T_{\lambda,\mu}$ and $\delta^{-1}T_{\eta,\theta}$, i.e.,

$$V = T_{\lambda,\mu} \cap \delta^{-1}T_{\eta,\theta}.$$

For $z \in V$, we have

$$z = t + \sigma = \delta^{-1}(t' + \sigma') \Longrightarrow \delta(t + \sigma) = t' + \sigma'$$

where $t' \in \mathbb{F}_q$ and $\sigma' = \eta + \theta\sigma_0$. Let $\delta = x_0 + x_1\sigma_0, x_0, x_1 \in \mathbb{F}_q$. According to the way we choose σ_0, we have $\sigma_0^2 = \sigma_0 + w, w \in \mathbb{F}_q$. Consequently, we have the following deviation:

$$\begin{aligned}
\delta(t + \sigma) &= (x_0 + x_1\sigma_0)(t + \lambda + \mu\sigma_0) \\
&= x_0(t + \lambda) + (x_0\mu + x_1 t + x_1\lambda)\sigma_0 + x_1\mu\sigma_0^2 \\
&= [x_0(t + \lambda) + x_1\mu w] + [x_0\mu + x_1(t + \lambda + \mu)]\sigma_0 \\
&\quad (\text{using } \sigma_0^2 = \sigma_0 + w) \\
&= t' + \sigma' = t' + \eta + \theta\sigma_0.
\end{aligned}$$

From the last two identities, we have

$$x_0\mu + x_1(t + \lambda + \mu) = \theta \tag{8}$$

$$x_0(t + \lambda) + x_1\mu w = t' + \eta. \tag{9}$$

Since $\delta \notin \mathbb{F}_q$, then $x_1 \neq 0$. From (8) and (9), $t = \frac{\theta + x_0\mu}{x_1} + \lambda + \mu$ and $t' = x_0(t + \lambda) + x_1\mu w + \eta$. Thus V has exactly one element $\Longrightarrow |V| = 1$. Thus $C_{\mathbf{a},\mathbf{b}}(\tau) = \pm q$ from (6).

Case 2. $\delta \in \mathbb{F}_q$. In this case,

$$\begin{aligned}
& f_{\lambda,\mu}(x) + f_{\eta,\theta}(\delta x) \\
= \; & f_j(Tr_n^{2n}(x)) + f_i(\delta Tr_n^{2n}(x)) + Tr_1^n(Tr_n^{2n}(\beta x)) \\
= \; & h(Tr_n^{2n}(x)) + Tr_1^n(Tr_n^{2n}(\beta x))
\end{aligned}$$

where $h(x)$ is defined in Theorem 2 and

$$\beta = \lambda + \mu\sigma_0 + (\eta + \theta\sigma_0)\delta.$$

The element $\beta \notin \mathbb{F}_q$ if and only if

$$\mu + \theta\delta \neq 0 \Longleftrightarrow \delta \neq \theta^{-1}\mu.$$

Thus, if $\delta \neq \theta^{-1}\mu$, then $\beta \notin \mathbb{F}_q$. Applying Property 1, it follows that

$$\begin{aligned} C_{\mathbf{a},\mathbf{b}}(\tau) + 1 &= \sum_{x \in \mathbb{F}_{q^2}} (-1)^{h(Tr_n^{2n}(x)) + Tr_1^n(Tr_n^{2n}(\beta x))} \\ &= \sum_{y,z \in \mathbb{F}_q} (-1)^{h(y) + Tr_1^n(z)} \text{ (here } q^{2-2} = 1) \\ &= 0. \end{aligned}$$

If $\delta = \theta^{-1}\mu$, then $\beta = \lambda + \eta \in \mathbb{F}_q$. Using the similar approach as the above and Property 1, we obtain that

$$C_{\mathbf{a},\mathbf{b}}(\tau) + 1 = q \sum_{y \in \mathbb{F}_q} (-1)^{h(y) + Tr_1^n(\beta y)} = q\widehat{h}(\beta)$$

which completes the proof.

□

We have the following remarks about the result of Theorem 2.

Remark 1 *(a) The out-of-phase autocorrelation of any sequence in the multiple bent function signal set is three valued: $\{-1, -1 \pm q\}$ and cross correlation of any pair of the sequences has the same three values except for one shift.*

(b) The result of Theorem 2 still holds for the case that all the f_i's are equal.

(c) If n is odd, the proof of Theorem 2 can be applied to the case for which g is an almost bent, i.e., the Hadamard transform of g has three values: 0 and $\pm 2^{\frac{n+1}{2}}$. In this case, there are $(q-1)$ signal sets each with parameters $(q^2-1, q, 2q+1)$, and the multiple signal sets have the same results in Theorem 2 except $-1 \pm q$ is replaced by $1 \pm 2q$. Thus, the maximum correlation of n odd is worse than that of n even.

From the proof and the result of Theorem 2, the following corollary is immediate.

Corollary 1 *Let $BF^+ = \cup_{i=0}^{q-2} S_i$. Then each sequence in BF^+ has the following trace representation:*

$$f_{\lambda,\mu}(x) = f_i(Tr_n^{2n}(x)) + Tr_1^N((\lambda + \mu\sigma_0)x),$$

where $\lambda \in \mathbb{F}_q, \mu = \omega^i \in \mathbb{F}_q^*$, and BF^+ is a $(q^2-1, q^2-q, q+1, q+1)$ low correlation zone signal set.

Remark 2 *Low correlation zone signal sets with period $q^l - 1$ ($q = 2^n$) from the other known constructions have the parameters $(q^l - 1, r, 1, \frac{q^l-1}{q-1})$ where $r \leq q - 1$ [21] [1] [2] [6]. All the constructions have the form of (3) and the size of such a signal set is determined by the number of shift-distinct row vectors of a $q \times q$ non-cyclic Hadamard matrix. Different sequences are constructed by taking shift-distinct row vectors of the Hadamard matrix as the functions g in (3) (see [6]).*

The result of Corollary 1 shows a trade-off between the correlation and the size of the signal sets. For the sequences with period $q^2 - 1$, the known constructions produce the low correlation zone signal sets with parameters $(q^2 - 1, r, 1, q + 1)$ where $r \leq q - 1$, i.e., the maximum correlation is equal to 1 and the size is $\leq q - 1$. On the other hand, the new signal set, given by Corollary 1, has parameters $(q^2-1, q(q-1), q+1, q+1)$ where maximum correlation is equal to $q+1$, which is worse than the known constructions (but it still optimal according to the bound in [22]), and the size is equal to $q(q-1)$, which is greater than or equal to q times as big as the sizes of the known constructions.

5 High Order Shift-Distinctness of the Multiple Bent Function Signal Sets

In this section, we discuss the high-order shift-distinct property of multiple bent function signal sets constructed in Section 4. First, if all the f_is are equal, we have the following result.

Theorem 3 *If $f_i = f, 0 \leq i < q - 1$, then $S_i, 0 \leq i < q - 1$ are pairwise shift distinct.*

In order to prove Theorem 3, we need the following result to determine whether two functions are equal. (The proof of the following lemma can be found in a finite field book, say [13][14] or in [4].)

Lemma 1 *Let $h(x) = \sum_{i=0}^{2^t-1} h_i x^i$ and $g(x) = \sum_{i=0}^{2^t-1} g_i x^i$ be two functions from $\mathbb{F}_{2^t}$ to $\mathbb{F}_2$, $h_i, g_i \in \mathbb{F}_{2^t}$, then $h(x) = g(x)$ if and only if $h_i = g_i, 0 \leq i < 2^t$. Furthermore, if we write both $h(x)$ and $g(x)$ in their trace representations, i.e., $h(x) = \sum_{i\in\Gamma} Tr_1^{t_i}(h_i x^i)$ and $g(x) = \sum_{i\in\Gamma} Tr_1^{t_i}(g_i x^i)$ where Γ is the set consisting of all coset leaders modulo $2^t - 1$, $t_i \,|\, t$, and $h_i, g_i \in \mathbb{F}_{2^{t_i}}$, then $h(x) = g(x)$ if and only if $h_i = g_i, \forall i \in \Gamma$, and $h(0) = g(0)$.*

Proof of Theorem 3. For a pair of sequences $\mathbf{a} \in S_i$ where $\theta = \omega^i$ and $\mathbf{b} \in S_j$ where $\mu = \omega^j$, if there is $0 \leq k < q^2 - 1$ such that $\mathbf{b} = L^k\mathbf{a}$, then we have

$$f_{\lambda,\mu}(x) = f_{\eta,\theta}(\delta x), \delta = \alpha^k.$$

which gives that

$$\begin{aligned} & f(Tr_n^{2n}(x)) + Tr_1^{2n}((\lambda + \mu\sigma_0)x) \\ = \;& f(Tr_n^{2n}(\delta x)) + Tr_1^{2n}((\eta + \theta\sigma_0)(\delta x). \end{aligned} \tag{10}$$

We may write

$$f(Tr_n^{2n}(x)) = \sum_{i=0}^{q^2-1} h_i x^i, h_i \in \mathbb{F}_{q^2}. \tag{11}$$

Since $f(x)$ is bent, then $f(x)$ is not linear. Therefore, there exists at least one i such that $h_i \neq 0$ and $H(i) > 1$ where $H(i)$ is the Hamming weight of the integer i. Together with (10), from one of those i's, by applying Lemma 1, we have

$$h_i x^i = h_i \cdot (\delta x)^i \Longrightarrow \delta = 1.$$

Substituting $\delta = 1$ into (10), we obtain

$$Tr_1^n((\lambda + \mu\sigma_0)x) = Tr_1^n((\eta + \theta\sigma_0)(x) \Longrightarrow \lambda + \mu\sigma_0 = \eta + \theta\sigma_0.$$

Since $\{1, \sigma_0\}$ is a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, the above identity implies that $\lambda = \eta$ and $\mu = \theta$ which contradicts with $\mu \neq \theta$. Thus S_i and S_j are shift distinct as long as $\mu \neq \theta \Longrightarrow i \neq j$.

□

Theorem 4 *The signal sets $S_i, 0 \leq i < q-1$ are third-order shift distinct.*

Due to lack of space, we won't give a complete proof for this result. Instead, we outline the proof as follows. We need to use some results of interleaved sequences (see [8][9][17]). In other words, we write any sequence in S_i as a $(q-1) \times (q+1)$ array where the first row of the array is the first $(q+1)$ elements of the sequence, the second row of the array is the second $(q+1)$ elements of the sequence, and so on. If $\mathbf{a} = L^s(\mathbf{b}) + L^t(\mathbf{c})$ where these three sequences belong to different signal sets S_i, S_j and S_k, then the columns in the array formed by $\mathbf{a}$ are equal to the corresponding columns of the array formed by $L^s(\mathbf{b}) + L^t(\mathbf{c})$. Using the fact that there is one zero column in each of these arrays, we can derive that two bent functions involved in $\mathbf{b}$ and $\mathbf{c}$ are shift equivalent, which contradicts the assumption. Thus, they are 3rd-order shift distinct.

Remark 3 *We can make the order of shift-distinctness of the multiple bent function signal sets very large using special bent functions. For example, if there exists $m > 3$ monomial bent functions $Tr_1^n(\beta_i x^{r_i}), \beta_i \in \mathbb{F}_q$ such that $\sum_{i=1}^m r_i > q$, we may choose f_vs as follows. Let $f_v(x) = Tr_1^n(\beta_i \omega^j x^{r_i})$ where $v = r_1 + r_2 + \cdots + r_i + j, v = 0, 1, \cdots, q-2$. Then $S_i, 0 \leq i < q-1$ are mth-order shift distinct. The results on this question will appear in the full paper.*

6 Conclusions

The pre-image set of nonzero Hadamard spectra of the sum of a composed function and a trace function from $\mathbb{F}_{q^l}$ to $\mathbb{F}_2$ is independent of the function involved in the composition. Using this property, multiple

bent function signal sets of period q^2-1 where n even are constructed from different bent functions in which each individual signal set is a bent function signal set. The correlation of any pair of sequences in the $(q-1)$ bent function signal sets of period q^2-1 is upper bounded by $q+1$ except for one shift. As a by-product, the union of the multiple bent function signal sets gives a low correlation zone signal set with parameters $(q^2-1, q(q-1), q+1, q+1)$. This construction provides a good trade-off between correlation and sizes. The multiple bent function signal sets are 3rd-order shift distinct. However, if all the $(q-1)$ bent functions involved in the construction are equal, then the multiple bent function signal set only satisfy the pairwise shift distinct property. By properly choosing bent functions, mth-order shift distinctness can be achieved where $m > 3$. High-order shift-distinct property directly connects with high-order correlation of sequences. It is not easy to compute high-order correlation of the sequences, although this is the case in real communication systems.

References

[1] 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.

[2] J.W. Jang, J.S. No, H.B. Chung, and X.H. Tang, New sets of optimal p-ary low correlation zone sequences, *IEEE Trans. Inform. Theory*, vol. 53, No. 2, pp. 815-821, February 2007.

[3] S.W. Golomb, *Shift Register Sequences,* Holden-Day, Inc., San Francisco, 1967, revised edition, Aegean Park Press, Laguna Hills, CA, (1982).

[4] S.W. Golomb and G. Gong, *Signal Design with Good Correlation: for Wireless Communications, Cryptography and Radar Applications*, Cambridge University Press, 2005.

[5] G. Gong, Constructions of multiple shift-distinct signal sets with low correlation, accepted by *2007 IEEE International Symposium on Information Theory (ISIT2007)*, 24th - 29th June 2007, Nice, France.

[6] G. Gong, S. W. Golomb, and H.Y. Song, A note on low correlation zone signal sets, *40the Annual Conference of Information Sciences and Systems (CISS 2006)*, March 22-24, 2006, Princeton University, Technical Co-Sponsorship With IEEE Information Theory Society. Technical Report, CACR 2006-06, University of Waterloo, January 2006. Submitted to *IEEE Trans. Inform. Theory*, and revised in April 2007.

[7] G. Gong, Correlation among signal sets, presented at the Special Session on *Coding Theory and Cryptography*, organized by Horacio Tapia-Recillas and Neal Koblitz, at *VI Joint Meeting of American Mathematical Society and Sociedad Matematica Mexicana (AMS-SMM)*, May 12-15, 2004, Huston.

[8] G. Gong, Theory and applications of q-ary interleaved sequences, *IEEE Trans. on Inform. Theory*, Vol. 41, No. 2, March 1995, pp. 400-411.

[9] G. Gong, New Designs for signal sets with low cross-correlation, balance property and large linear span: $GF(p)$ Case, *IEEE Trans. on Inform. Theory*, Vol. 48, No.11, November 2002, pp. 2847-2867.

[10] A. Klapper, A.H. Chan, and M. Goresky, Cross-correlations of linearly and quadratically related geometric sequences and GMW sequences, *Discrete Appl. Math.* **46**, No. 1, (1993), pp. 1-20.

[11] P.V. Kumar, On bent sequences and generalized bent functions, Ph. D. Thesis, University of Southern California, Los Angeles, 1983.

[12] T. Helleseth and P.V. Kumar, Sequences with low correlation, a chapter in *Handbook of Coding Theory*, edited by V. Pless and C. Huffman, Elsevier Science Publishers, 1998, pp. 1765-1853.

[13] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Volume 20, Addison-Wesley, (1983). (Revised version, Cambridge University Press, 1997.)

[14] R.J. McEliece, *Finite Fields for Computer Scientists and Engineers*, The Knuwer International Series in Engineering and Compute Science, Vol. 23, Kluwer Academic Publishers, Boston, (1986).

[15] N. Y. Yu and G. Gong, Higher order autocorrelation of binary sequences with ideal two-level autocorrelation, *Proceedings of Canadian Workshop on Information Theory (CWIT'05)*, pp. 391 - 394, Montreal, Canada, June 5-8, 2005.

[16] J.D. Olsen, R.A. Scholtz and L.R. Welch, Bent-function sequences, *IEEE Trans. Inform. Theory*, Vol. 28, No. 6, November 1982, pp. 858-864.

[17] K.G. Paterson, Binary sequence sets with favorable correlations from difference sets and MDS codes, *IEEE Trans. Inform. Theory*, Vol. 44, No. 1, January 1998, pp. 172-180.

[18] M.B. Pursley, *Introduction to Digital Communications*, Pearson Prentice Hall, 2005.

[19] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, *Spread Sprectrum Communications Handbook*, McGraw-Hill Companies, Inc., 2002.

[20] A.J. Viterbi, *CDMA − Principles of Spread Spectrum Communication*, Reading, MASS., Addison-Wesley, 1995.

[21] 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.

[22] X. H. Tang, P. Z. Fan and S. matsufuji, Lower bounds on correlation of spreading sequence sets with low or zero correlation zone, *Electronic Letters*, vol. 36, No. 6, pp. 551-552, March, 2000.

[23] N. Zierler, Linear recurring sequences, *J. Soc. Indust. Appl. Math.* **7** , (1959), pp. 31-48.