Front. Electr. Electron. Eng. China (2006) 3: 340–344
DOI 10.1007/s11460-006-0045-9

RESEARCH ARTICLE

KE Pin-hui, CHANG Zu-ling, WEN Qiao-yan

Construction of generalized binary Bent sequences

Abstract Bent functions in trace forms play an important role in the constructions of generalized binary Bent sequences. Trace representation of some degree two Bent functions are presented in this paper. A sufficient and necessary condition is derived to determine whether the sum of the combinations of Gold functions, $\mathrm{tr}_1^n(\boldsymbol{x}^{2^i+1})$, $1 \le i \le n-1$, over finite fields F_{2^n} (n be even) in addition to another term $\mathrm{tr}_1^{n/2}(x^{2n/2+1})$ is a Bent function. Similar to the result presented by Khoo et al., the condition can be verified by polynominal greatest common divisor (GCD) computation. A similar result also holds in the case F_{p^n} (n be even, p be odd prime). Using the constructed Bent functions and Niho type Bent functions given by Dobbertin et al., many new generalized binary Bent sequences are obtained.

Keywords generalized Bent sequences, Bent functions, and finite fields

1 Introduction

Bent functions have been applied in many areas including coding theory (Reed-Muller code) and cryptography (Stream Cypher) since they were introduced by Rothaus in 1976 [1]. Especially, Olsen et al. constructed families of sequences with good properties by using Bent function, and Bent sequences, whose out-of-phase autocorrelation and cross-correlation values reach the Welch bound asymptotically. These families of sequences can be applied in many communication system such as code-division multiple-access (CDMA), radar and so on. NO et al. [2] generalized the notations of Bent sequences by defining a modified trace transform and presented a large class of generalized binary Bent sequences. Compared with Bent sequences, generalized binary Bent sequences have the merit of being simpler in expression. More importantly, we can get more balanced sequences with good correlation properties by lifting ideas [2]. So it is valuable for us to get more classes of generalized binary Bent sequences.

Bent functions defined in the intermediate field play an important role in the construction of generalized binary Bent functions, making them necessary. On the other hand, Bent functions with simple expressions (represented by trace functions) are required to have simpler forms so as to make the resulting generalized binary Bent sequences have simple forms. Although from the point of theory, Boolean functions on F_2^n, polynomial functions on F_{2^n}, sequences with period dividing 2^n-1 over F_2 are one-to-one [3]. One can also get the trace representation of a Boolean function over F_{2^n} in theory. But it is always difficult for us to get an exact trace representation. For example, Kim et al. [10] got the trace representations of partial spread (PS) class Bent functions. Thus, it is important to get the trace representations of Bent functions known and to build new classes of Bent functions.

There are two classes of well-known Bent functions. One class is the maiorana-macfarland (MM) class and another is the PS class. Naturally it is easy to get the Bent functions defined in the intermediate fields from these two classes. No et al. [2] considered the two cases and constructed two classes of generalized Bent sequences. Khoo et al. [4] presented a necessary and sufficient condition of Semi-Bent function which is the linear combinations of Gold functions

Translated from *Journal on Communications*, 2005, 26(12): 19–23 (in Chinese)

KE Pin-hui(✉)
School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China
E-mail: keph@eyou.com

CHANG Zu-ling
State Key Laboratory of Information Security,
Chinese Academy of Sciences, Beijing 100039, China
Department of Mathematics, Zhengzhou University,
Zhengzhou 450025, China

WEN Qiao-yan
School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

$\mathrm{tr}_1^n(x^{2^i+1})$ over F_2. They also proved that the condition can be efficient verified by computing some polynomials' GCD. Then, they generalized these results to the field F_{p^n}, where p is odd prime and n is odd integer. Dobbertin et al. [5] obtained some new classes of Bent functions by using Niho type power function.

In this paper, some trace representations of Bent functions of degree two are presented. We conclude that the linear combination of Gold functions $\mathrm{tr}_1^n(x^{2^i+1})$ over F_{2^n} (n be even) cannot be Bent functions. We also obtain the sufficient and necessary condition of the linear combination above being Bent functions when they are added with another term $\mathrm{tr}_1^{n/2}(x^{2n/2+1})$. Smilar to the result in [2], this condition can be verified by computing the polynomials' GCD. This result can be generalized to the case F_{p^n} (n be even, p be odd). Then by using the obtained Bent functions and the Bent functions presented in [5], we construct more new families of generalized binary Bent sequences.

2 Basic definitions and notations

Let F_{2^n} be a finite field of order 2^n and $V_{2^n}^k$ be a vector space over F_{2^n}. And Let $\mathrm{tr}_1^n(\boldsymbol{x}) = \boldsymbol{x} + \boldsymbol{x}^2 + \cdots + \boldsymbol{x}^{2^{n-1}}$ denote the trace function from F_{2^n} to F_2.

Definition 1 Let $f(\boldsymbol{x})$ be a function from $V_{2^n}^k$ to F_2, then we call

$$\widehat{f}(\boldsymbol{\lambda}) = \frac{1}{\sqrt{2^{nk}}} \sum_{\boldsymbol{x} \in V_{2^n}^k} (-1)^{f(\boldsymbol{x}) + \mathrm{tr}_1^n(\boldsymbol{\lambda} \cdot \boldsymbol{x}^{\mathrm{T}})}$$

the trace transform of $f(\boldsymbol{x})$, here $\boldsymbol{\lambda} \in V_{2^n}^k$ and $\boldsymbol{\lambda} \cdot \boldsymbol{x}^{\mathrm{T}} = \sum_{i=1}^{k} \lambda_i x_i$.

Obviously, in the case $n = 1$, the trace transform defined above is just the Walsh-Hadamard transform. In general, for an even integer n, there exists a self-dual basis $\{\alpha_i\}_{i=1}^n$ of F_{2^n} over F_2 [6]. Suppose

$$x_i = \sum_{j=1}^{n} x_{ij}\alpha_j \quad \text{and} \quad \lambda_i = \sum_{j=1}^{n} \lambda_{ij}\alpha_j, \ 1 \le i \le n,$$

then $f(\boldsymbol{x})$ can be seen as a Boolean function from V_2^{nk} to F_2. And we have

$$\mathrm{tr}_1^n(\boldsymbol{\lambda} \cdot \boldsymbol{x}^{\mathrm{T}}) = \sum_{i=1}^{k} \mathrm{tr}_1^n(x_i\lambda_i) = \sum_{i=1}^{k}\sum_{j=1}^{n} x_{ij}\lambda_{ij}$$

So the trace transform of $f(\boldsymbol{x})$ is equivalent to the Walsh-Hadamard transform of Boolean functions with nk input variable.

Definition 2 Let $f(\boldsymbol{x})$ be a function from $V_{2^n}^k$ to F_2, if $\left|\widehat{f}(\boldsymbol{\lambda})\right| = 1$, when $\boldsymbol{\lambda} \in V_{2^n}^k$, then we call $f(\boldsymbol{x})$ a Bent function over $V_{2^n}^k$.

3 Some new characterization of degree two Bent functions

Let f be a function from F_2^n to F_2. By Parseval's theorem, the maximum Walsh spectrum of f is at least $2^{n/2}$. When n is even, Bent functions achieve this lowest bound. For a general n, it is difficult for us to characterize all the functions whose maximum Walsh spectrum achieve the lower bound. But in the case where n is even and the algebraic degree is two, all functions that achieve this bound is known [7]. For $f: F_2^n \to F_2$, it corresponds to function from F_{2^n} to F_2 by taking a basis of F_{2^n} over F_2. So we can consider the same question over F_{2^n}. It is obvious that all the Boolean functions of degree two have the form $f(\boldsymbol{x}) = \sum_{\{i:w(e_i)\le 2\}} \mathrm{tr}(\beta_i \boldsymbol{x}^{e_i})$, here $\omega(e_i)$ denotes the weight of e_i (the number of 1 in its binary expression). Khoo et al. [4] have considered the necessary condition when the linear combination of Gold function can form Semi-Bent function in the case of F_{2^n} in which n is odd, and also the necessary condition when the linear combination of Gold function can form Semi-Bent function and Bent function in the case of F_{p^n} and p are odd prime numbers and n is odd.

Now Let us consider the case F_{2^n} when n is even. Although they are all degree two Bent functions and their construction and enumeration are well known, we wish the Bent function to have a simple trace representation over the field, in order to have the generalized binary Bent sequences have a simple representation, as we have stated in the introduction. We hope some Bent functions of degree two (at least a part of them) can be simply represented by trace function. we find that the linear combinations of Gold functions can not be Bent functions (also see the note following Theorem 1), but we have the following result:

Theorem 1 Let $n = 2m$, $M = 2^m + 1$, m be even, $c_i \in \{0,1\}$, $1 \le i \le m-1$, define

$$f(\boldsymbol{x}) = \sum_{i=1}^{m-1} c_i \mathrm{tr}_1^n(\boldsymbol{x}^{1+2^i}) + \mathrm{tr}_1^m(\boldsymbol{x}^M)$$

then f is Bent function from F_2^n to F_2 if

$$L = \begin{pmatrix} c_0 & c_1 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & \cdots & c_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ c_1 & c_2 & \cdots & c_0 \end{pmatrix}$$

have full rank, here $c_0 = 0$, $c_m = 1$, $c_i = c_{n-i}$ and

$1 \le i \le m-1$.

Proof It is easy to know that functions defined above correspond to Boolean function of degree two. So we can verify the function by considering the rank of its symplectic form $B_f(\boldsymbol{x},\boldsymbol{z}) = f(\boldsymbol{x}) + f(\boldsymbol{z}) + f(\boldsymbol{x}+\boldsymbol{z})$. By

$$\begin{aligned}
B_f(\boldsymbol{x},\boldsymbol{z}) &= f(\boldsymbol{x}) + f(\boldsymbol{z}) + f(\boldsymbol{x}+\boldsymbol{z}) = \sum_{i=1}^{m-1} c_i \mathrm{tr}_1^n(\boldsymbol{x}^{1+2^i}) \\
&+ \mathrm{tr}_1^m(\boldsymbol{x}^M) + \sum_{i=1}^{m-1} c_i \mathrm{tr}_1^n(\boldsymbol{z}^{1+2^i}) + \mathrm{tr}_1^m(\boldsymbol{z}^M) \\
&+ \sum_{i=1}^{m-1} c_i \mathrm{tr}_1^n((\boldsymbol{x}+\boldsymbol{z})^{1+2^i}) + \mathrm{tr}_1^m((\boldsymbol{x}+\boldsymbol{z})^M) \\
&= \sum_{i=1}^{m-1} c_i \mathrm{tr}_1^n(\boldsymbol{z}\boldsymbol{x}^{2^i} + \boldsymbol{x}\boldsymbol{z}^{2^i}) + \mathrm{tr}_1^m(\boldsymbol{z}\boldsymbol{x}^{2^m} + \boldsymbol{x}\boldsymbol{z}^{2^m}) \\
&= \sum_{i=1}^{m-1} c_i \mathrm{tr}_1^n(\boldsymbol{z}\boldsymbol{x}^{2^i}) + \sum_{i=1}^{m-1} c_i \mathrm{tr}_1^n((\boldsymbol{z}\boldsymbol{x}^{2^i})^{2^{n-i}}) + \mathrm{tr}_1^m(\mathrm{tr}_m^n(\boldsymbol{x}\boldsymbol{z}^{2^m})) \\
&= \sum_{i=1}^{m-1} c_i \mathrm{tr}_1^n(\boldsymbol{x}\boldsymbol{z}^{2^i}) + \sum_{i=1}^{m-1} c_i \mathrm{tr}_1^n(\boldsymbol{x}\boldsymbol{z}^{2^{n-i}}) + \mathrm{tr}_1^m(\mathrm{tr}_m^n(\boldsymbol{x}\boldsymbol{z}^{2^m})) \\
&= \mathrm{tr}_1^n(\boldsymbol{x}(c_1\boldsymbol{z}^2 + c_2\boldsymbol{z}^{2^2} + \cdots + c_{m-1}\boldsymbol{z}^{2^{m-1}} + \boldsymbol{z}^{2^m} + c_{m-1}\boldsymbol{z}^{2^{m+1}} \\
&+ \cdots + c_1\boldsymbol{z}^{2^{n-1}})),
\end{aligned}$$

$B_f(\boldsymbol{x},\boldsymbol{z}) = 0$ holds for any $\boldsymbol{x} \in F_{2^n}$ if and only if $L(\boldsymbol{z}) = c_1\boldsymbol{z}^2 + c_2\boldsymbol{z}^{2^2} + \cdots + c_{m-1}\boldsymbol{z}^{2^{m-1}} + \boldsymbol{z}^{2^m} + c_{m-1}\boldsymbol{z}^{2^{m+1}} + \cdots + c_1\boldsymbol{z}^{2^{n-1}} = 0$

It is easy to see that $L(\boldsymbol{z})$ is a linearized polynomial over F_{2^n}. By [9], the root number of $L(\boldsymbol{z})$ is determined by a coefficient matrix of $L(\boldsymbol{z})$ with respect to a basis $\{\alpha^{2^i}\}_{i=0}^{n-1}$ of F_2^n over F_2

$$\boldsymbol{L} = \begin{pmatrix} c_0 & c_1 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & \cdots & c_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ c_1 & c_2 & \cdots & c_0 \end{pmatrix}$$

So $\boldsymbol{L}(\boldsymbol{z})$ only has a root of zero if and only if $\boldsymbol{L}$ has full rank. In this situation, the rank of the sympletic form of $f(\boldsymbol{x})$ is n. Therefore $f(\boldsymbol{x})$ is a Bent function. The proof is thus completed.

Note Because $\mathrm{tr}_1^n((x^{2^i+1})^{2^{n-i}}) = \mathrm{tr}_1^n(x^{2^{n-i}+1})$ and $\mathrm{tr}_1^n(x^M) = \mathrm{tr}_1^m(\mathrm{tr}_m^n(x^M)) = 0$, we only need to consider the linear combination of the former $m-1$ term of Gold function. Furthermore, if $f(\boldsymbol{x}) = \sum_{i=1}^{m-1} c_i \mathrm{tr}_1^n(x^{1+2^i})$, which means that $f(\boldsymbol{x})$ is the linear combination of the Gold function. By the proof of Theorem 1, we have

$$\boldsymbol{L} = \begin{pmatrix} 0 & c_1 & \cdots & c_{m-1} & 0 & c_{m-1} & \cdots & c_1 \\ c_1 & 0 & \cdots & c_{m-2} & c_{m-1} & c_0 & \cdots & c_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ c_1 & c_2 & \cdots & 0 & c_{m-1} & c_{m-2} & \cdots & 0 \end{pmatrix}$$

It is easy to verifiy that $\boldsymbol{L}$ can not have full rank (the sum of row is zero). In this case, $f(\boldsymbol{x})$ can not be a Bent function. It can also enable us to understand that the case F_{2^n}, in which n is even, is not included in [4].

Similar to the discussion in [4], $\boldsymbol{L}$ is cyclic matrix and its generation matrix can generate a cyclic code. Denote it as *C*. Let

$$C(\boldsymbol{x}) = \sum_{i=1}^{m-1} c_i(\boldsymbol{x}^i + \boldsymbol{x}^{n-i}) + \boldsymbol{x}^m$$

and

$$g(\boldsymbol{x}) = (C(\boldsymbol{x}), \boldsymbol{x}^n + 1)$$

is the generation polynomial of *C*, then the rank of *C* is $n - \deg(g(\boldsymbol{x}))$. So Rank $(\boldsymbol{L}) = n$ if and only if $(C(\boldsymbol{x}), \boldsymbol{x}^n + 1) = 1$. Thus we have:

Theorem 2 Let n, M and $f(\boldsymbol{x})$ be defined as Theorem 1, then $f(\boldsymbol{x})$ is a Bent function if and only if $(C(\boldsymbol{x}), \boldsymbol{x}^n + 1) = 1$, in which $C(\boldsymbol{x}) = \sum_{i=1}^{m-1} c_i(\boldsymbol{x}^i + \boldsymbol{x}^{n-i}) + \boldsymbol{x}^m$.

Corollary 1 Let $n = 2^e$, e be an integer greater than 1. Then for any $c_i \in \{0,1\}, 1 \le i \le m-1$, $f(\boldsymbol{x}) = \sum_{i=1}^{m-1} c_i \mathrm{tr}_1^n(\boldsymbol{x}^{1+2^i}) + \mathrm{tr}_1^m(\boldsymbol{x}^M)$ is a Bent function.

Proof For $(C(\boldsymbol{x}), \boldsymbol{x}^n + 1) = (C(\boldsymbol{x}), \boldsymbol{x} + 1) = 1$ and Theorem 2, the corollary above holds.

Corollary 2 [2] Let $n = 2m$, $M = 2^m + 1$, m be positive integer, then $f(\boldsymbol{x}) = \mathrm{tr}_1^m(r\boldsymbol{x}^M)$ is a Bent function, here $r \in F_{2^m}^*$.

Proof Let α be the primitive generator of F_{2^n}, then α^M is the generation of F_{2^m}. Suppose $r = \alpha^{Mt}$, then

$$\hat{f}(\boldsymbol{\lambda}) = \frac{1}{2^m} \sum_{\boldsymbol{x} \in F_{2^n}} (-1)^{\mathrm{tr}_1^n(r\boldsymbol{x}^M) + \mathrm{tr}_1^n(\boldsymbol{\lambda}\boldsymbol{x})} = \frac{1}{2^m} \sum_{\boldsymbol{x} \in F_{2^n}} (-1)^{\mathrm{tr}_1^n(\boldsymbol{x}^M) + \mathrm{tr}_1^n(\boldsymbol{\lambda}\alpha^{-t}\boldsymbol{x})}$$

Because the polynomial corresponding to $\mathrm{tr}_1^m(\boldsymbol{x}^M)$ is $C(\boldsymbol{x}) = \boldsymbol{x}^m$, so $(C(\boldsymbol{x}), \boldsymbol{x}^n + 1) = 1$, and by Theorem 2, we know $\mathrm{tr}_1^m(\boldsymbol{x}^M)$ is a Bent function. Thus for any $r \in F_{2^m}^*$, $\mathrm{tr}_1^m(r\boldsymbol{x}^M)$ is a Bent function.

Corollary 3 [8] Let $n = 2m, M = 2^m + 1$, m be positive integer, then $f(\boldsymbol{x}) = \sum_{i=1}^{m-1} \mathrm{tr}_1^n(x^{1+2^i}) + \mathrm{tr}_1^m(\boldsymbol{x}^M)$ is a Bent function over F_{2^n}.

Proof By $(C(\boldsymbol{x}), \boldsymbol{x}^n + 1) = (\boldsymbol{x} + \boldsymbol{x}^2 + \cdots + \boldsymbol{x}^{n-1}, \boldsymbol{x}^n + 1) = (1 + \boldsymbol{x} + \boldsymbol{x}^2 + \cdots + \boldsymbol{x}^{n-2}, 1 + \boldsymbol{x} + \boldsymbol{x}^2 + \cdots + \boldsymbol{x}^{n-1}) = 1$ and Theorem 2, we know that $f(\boldsymbol{x})$ is Bent function. Theorem 2 can be generalized to the case F_{p^n}, where p is an odd prime number and n is even. Although this case has no relation with the construction of generalized binary Bent sequences, it is still written out for the sake of integrity.

Let $f: F_{p^n} \to F_p$, denote

$$\hat{f}(\boldsymbol{\lambda}) = \frac{1}{\sqrt{p^n}} \sum_{\boldsymbol{x} \in F_{p^n}} U^{\mathrm{tr}_1^n(\lambda \boldsymbol{x}) - f(\boldsymbol{x})}$$

here $U = \exp(2\pi i / p)$ is the identity root of p degrees. We call f a generalized Bent if $|\hat{f}(\boldsymbol{\lambda})| = 1$ for any $\boldsymbol{\lambda} \in F_{p^n}$.

Theorem 3 Let $n = 2m, M = 2^m + 1$, m be positive integer, $c_i \in F_{p^n}$, $1 \le i \le m-1$, define $f(\boldsymbol{x}) = \sum_{i=1}^{m-1} c_i \mathrm{tr}_1^n(\boldsymbol{x}^{1+p^i}) + \mathrm{tr}_1^m(\boldsymbol{x}^M)$ then f is generalized Bent if and only if $(c(\boldsymbol{x}), \boldsymbol{x}^n - 1) = 1$ and $c(\boldsymbol{x}) = \sum_{i=1}^{m-1} c_i(\boldsymbol{x}^i + \boldsymbol{x}^{n-i}) + \boldsymbol{x}^m$. Because the Proof is similar to that of Theorem 2, we omit it here.

4 Construction of generalized binary Bent sequences

By using the Bent function presented above and the Bent function constructed in [5], we constructed some new generalized binary Bent sequences.

Let $h = 2n = 4mk$ and $\{\beta_i\}_{i=1}^k$ be a basis of F_{2^n} over $F_{2^{2m}}$. Define $\varphi(\boldsymbol{x}) = \{\mathrm{tr}_{2m}^h(\beta_1 \sigma \boldsymbol{x}), \cdots, \mathrm{tr}_{2m}^h(\beta_k \sigma \boldsymbol{x})\}$, here $\sigma \in F_{2^h} \setminus F_{2^n}$. Then $\varphi(\boldsymbol{x})$ is linear onto mapping from F_{2^h} to $V_{2^{2m}}^k$.

Lemma 1 [2] Let $h = 2n = 4mk$, $\delta \in F_{2^n}^*$, $f(\boldsymbol{x})$ be a Bent function over $V_{2^{2m}}^k$ and $\varphi(\boldsymbol{x})$ is defined above. Then

$$S = \{s_\eta(t) \mid \eta \in F_{2^n}, 0 \le t \le 2^h - 2\}$$

$$s_\eta(t) = f(\varphi(\alpha^t)) + \mathrm{tr}_1^h((\eta\sigma + \delta)\alpha^t)$$

is a family of balanced generalized binary Bent sequences with out-of-phase autocorrelation and cross correlation $\{-2^m - 1, -1, 2^m - 1\}$.

Let $n = 2m$, then $\mathrm{tr}_1^n(\boldsymbol{x}) = \boldsymbol{x} + \bar{\boldsymbol{x}}$, here $\bar{\boldsymbol{x}} = \boldsymbol{x}^{2^m}$.

Theorem 4 [5] Let $f(\boldsymbol{x}) = \mathrm{tr}_1^n(\alpha \boldsymbol{x}^{d_1} + \boldsymbol{x}^{d_2})$, here $\alpha, \boldsymbol{x} \in F_{2^n}$. If $\alpha + \bar{\alpha} = 1$, then f in following cases:

1) $d_1 = 2^m + 1, d_2 = 3 \times 2^{m-1} - 1$;
2) $d_1 = 2^m + 1, d_2 = 2^m + 3$, m be odd;
3) $d_1 = 2^m + 1, d_2 = \frac{2^m + 5}{3}$, m be even

are all Bent functions. Here d_i satisfies that $\boldsymbol{x}^{d_i}$ is linear on F_{2^m}. We call it Niho type power exponent.

Theorem 5 Let $n = 2mk, M = 2^m + 1$ and n, m, k be positive integers. If $f(\boldsymbol{x})$ is a Bent function over $F_{2^{2m}}$, then $f(\boldsymbol{x}) = \sum_{i=1}^k f(\boldsymbol{x}_i)$ is a Bent function over $V_{2^{2m}}^k$.

Proof It is easy to prove by the definition of trace transform.

Theorem 6 Let $h = 2n = 4mk$, $M = 2^m + 1$ and m, k be positive integers.

$$S = \{s_\eta(t) \mid \eta \in F_{2^n}, 0 \le t \le 2^h - 2\}$$

1) If

$$f(\boldsymbol{x}) = \sum_{i=1}^{m-1} c_i \mathrm{tr}_1^n(\boldsymbol{x}^{1+2^i}) + \mathrm{tr}_1^m(\boldsymbol{x}^M)$$

here $c_i \in \{0,1\}$, and $(C(\boldsymbol{x}), \boldsymbol{x}^{2m} + 1) = 1$

here $C(\boldsymbol{x}) = \sum_{i=1}^{m-1} c_i(\boldsymbol{x}^i + \boldsymbol{x}^{n-i}) + \boldsymbol{x}^m$, then

$$s_\eta(t) = \sum_{i=1}^k \{\sum_{j=1}^{m-1} c_j \mathrm{tr}_1^{2m}(\mathrm{tr}_{2m}^h(\beta_i \sigma \boldsymbol{x})^{1+2^j})\} + \mathrm{tr}_1^m((\mathrm{tr}_{2m}^h(\beta_i \sigma \boldsymbol{x})^M)) + \mathrm{tr}_1^h((\eta\sigma + \delta)\boldsymbol{\alpha}^t)$$

2) If

$$f(\boldsymbol{x}) = \mathrm{tr}_1^{2m}(\alpha \boldsymbol{x}^{d_1} + \boldsymbol{x}^{d_2}),$$

here, $\boldsymbol{\alpha}, \boldsymbol{x} \in F_{2^{2m}}$, $\boldsymbol{\alpha} + \bar{\boldsymbol{\alpha}} = 1$, and d_i, $i = 1,2$ belong to the three cases of Theorem 4, then

$$s_\eta(t) = \sum_{i=1}^k \{f(\mathrm{tr}_{2m}^h(\beta_i \sigma \boldsymbol{x}))\}$$

are families of balanced generalized binary Bent sequences with out-of-phase autocorrelation and cross correlation $\{-2^m - 1, -1, 2^m - 1\}$.

Proof By Theorems 2, 4, 5 and Lemma 1, it is easy to prove.

By Theorem 6, we can construct more generalized binary Bent sequences.

5 Conclusions

Some trace representations of Bent functions of degree two are presented in this paper. The necessary and sufficient condition of linear combinations of Gold function being Bent functions when they are added with another term $\mathrm{tr}_1^{n/2}(\boldsymbol{x}^{2^{n/2}+1})$. Our results perfect the work in [4]. By using the Bent function obtained and the Bent functions constructed by Dobbertin et al. [5], we construct more new families of generalized binary Bent functions. We also see that the Bent functions used in the constructions are the generalization of Bent functions over finite field into multi-dimension field. Thus trace representation of Bent functions and construction of Bent functions are valuable.

Acknowledgements This work was supported by the National Natural Science Foundation of China (No.60373059), the National Research Foundation for the Doctoral Program of Higher Education of China (No.20040013007) and the Research Foundation of the State Key Laboratory of Information Security.

References

1. Rothaus O. S., On Bent functions, Jouranl of Combinatorial

Theory A, 1976, 20: 300–305
2. No J. S., Gil G. Mi, Shin D. J., Generalized Construction of binary Bent sequences with optimal correlation property, IEEE Trans. Inform. Theory, 2003, 49(7): 1769–1780
3. Youssef A. M., Gong G., Hyper-Bent functions, EUROCRYPT'01, LNCS, 2001: 406–419
4. Khoo K., Gong G., Stison D. R., A new characterization of Gold-like sequences, IEEE International symposium on Information Theory(ISIT), Lausanne, Switzerland , 2002, 181
5. Dobbertin H., Leander G., Canteaut A. et al, Construction of Bent functions via Niho power functions, preprint, 2004
6. Lempel A., Matrix factorization over GF(2) and trace-orthogonal bases of GF(2^n), SIAM J. Comput., 1975, 4(2): 175–186
7. Ding Cun-sheng, Xiao Guo-zhen, Stream Cypher, Beijing: Defence Industrial Publisher. 1994 (in chinese)
8. Kim S. H., No J. S., New family of binary sequences with three-valued crosscorrelation property, IEEE Trans. on Info. Theory, 2003, 49(11): 3054–3065
9. Lidle R., Niederreiter H., Finite Fields, Addison-wesley Pubilshing Company, 1983
10. Kim S. H., Gil G. M., Kim K. H., No J. S., Generalized Bent functions constructed from partial spreads, 2002, IEEE International Symposium on Inferences Theory, 2003, 49(11): 41