IEICE TRANS. FUNDAMENTALS, VOL.E87–A, NO.2 FEBRUARY 2004

PAPER

New Classes of Bent Functions and Generalized Bent Functions*

Sunghwan KIM[†a)], ***Student Member***, **Gang-Mi GIL**[††b)], ***and*** **Jong-Seon NO**[†c)], ***Nonmembers***

SUMMARY In this paper, a new class of bent functions is constructed by combining class M and class C bent functions. Using the construction method of the class D bent functions defined on the binary vector space, new p-ary generalized bent functions are also introduced for odd prime p.

key words: *bent functions, Boolean functions, generalized bent functions*

1. Introduction

A Boolean function from the n-dimensional binary vector space to the finite field F_2 is called a *bent function* if its Fourier coefficients only take the values $+1$ or -1, which was introduced by Rothaus [12]. The bent functions have been used in many areas such as constructions of families of binary sequences with the optimal correlation [7], [8], [11], error correcting codes [10], and cryptology [15], because they have good Fourier transform property.

There have been many research results on the bent functions [2], [3], [10]. One of the well-known classes of bent functions is called Maiorana-McFarland bent function, referred to as class M. Dillon constructed elementary Hadamard difference sets by using the partial spreads for a group of square order, whose characteristic functions correspond to bent functions, termed class PS (PS− and PS+) [4]. Two new classes of bent functions are introduced by Carlet, which are called class D and class C [2]. He also showed that all the bent functions have the property of generalized partial spread (GPS) [3]. Dobbertin introduced a new construction method of the normal bent functions by using a mapping, called bent triple [5]. He also showed that his construction includes the class M bent functions and the class PS− bent functions. Kumar, Scholtz, and Welch introduced generalized bent functions from the q-ary n-dimensional vector space to the set of integers modulo q, whose Fourier coefficients all have unit magnitude [7]. They constructed several generalized bent functions and proved the condition of n and q for which generalized bent functions exist. Kim, Gang, Kim, and No generalized PS− bent functions to construct p-ary generalized bent functions for odd prime p [6].

Remainder of the paper is organized as follows. Section 2 refers several known classes of bent functions. Section 3 introduces a new class of bent functions constructed by combining class M and class C bent functions. Section 4 presents new p-ary generalized bent functions for odd prime p using the construction method of the class D bent functions defined on the binary vector space.

2. Preliminaries

Let V_2^n be the n-dimensional vector space over the finite field F_2. Then a bent function is defined as follows.

Definition 1: *[Rothaus [12]] : A function $f(\underline{x})$ from V_2^n to F_2 is called bent if the Fourier transform of $f(\underline{x})$ only takes on the values $+1$ or -1, where the Fourier transform of $f(\underline{x})$ is given as*

$$F(\underline{\lambda}) = \frac{1}{\sqrt{2^n}} \sum_{\underline{x} \in V_2^n} (-1)^{f(\underline{x}) + \underline{\lambda} \cdot \underline{x}^{\mathrm{T}}}$$

where $\underline{x}^{\mathrm{T}}$ stands for the transpose of $\underline{x}$ and $\underline{\lambda} \cdot \underline{x}^{\mathrm{T}}$ denotes the inner product of the two row vectors $\underline{\lambda}$ and $\underline{x}$. □

Let F_{p^n} be the finite field with p^n elements. Let $n = em > 1$ for some positive integers e and m. Then the trace function $tr_m^n(\cdot)$ is the mapping from F_{p^n} to its subfield F_{p^m} defined by [9]

$$tr_m^n(x) = \sum_{i=0}^{e-1} x^{p^{mi}}$$

where x is an element in F_{p^n}.

Olsen, Scholtz, and Welch introduced the trace transform for a function from F_{2^n} to F_2 as follows.

Definition 2: *[Olsen, Scholtz, and Welch [11]] : Let $f(x)$ be a function from F_{2^n} to F_2. The trace transform of $f(x)$ is defined as*

$$\begin{aligned} \hat{F}(\lambda) &= (-1)^{\tilde{f}(\lambda)} \\ &= \frac{1}{\sqrt{2^n}} \sum_{x \in F_{2^n}} (-1)^{f(x) + tr_1^n(\lambda x)}, \quad \text{all } \lambda \in F_{2^n} \end{aligned}$$

and its inverse trace transform is given as

$$(-1)^{f(x)} = \frac{1}{\sqrt{2^n}} \sum_{\lambda \in F_{2^n}} \hat{F}(\lambda)(-1)^{tr_1^n(\lambda x)},$$

all $x \in F_{2^n}$. □

Manuscript received April 23, 2003.
Manuscript revised September 5, 2003.
Final manuscript received October 22, 2003.

[†]The authors are with School of EECS, Seoul National University, Seoul 151-742, Korea.
[††]The author is with Samsung Electronics, Suwon, Korea.
a) E-mail: nodoubt@ccl.snu.ac.kr
b) E-mail: cominkil@orgio.net
c) E-mail: jsno@snu.ac.kr

*This work was supported in part by BK21 and ITRC program of the Korean Ministry of Information and Communications.

The elements x and λ in F_{2^n} can be determined from the elements $\underline{x}$ and $\underline{\lambda}$ in V_2^n by the relations

$$\begin{aligned} x &= x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n \\ &\iff \underline{x} = (x_1, x_2, \cdots, x_n) \\ \lambda &= \lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n \\ &\iff \underline{\lambda} = (\lambda_1, \lambda_2, \cdots, \lambda_n) \end{aligned} \tag{1}$$

where x_i and λ_i are in F_2 and $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ is a basis of F_{2^n} over F_2. By replacing x in F_{2^n} by $\underline{x}$ in V_2^n, the function $f(x)$ from F_{2^n} to F_2 can be transformed into the corresponding Boolean function $f(\underline{x})$ from V_2^n to F_2.

In this section, as a trace transform of $f(x)$, both $\hat{F}(\lambda)$ and $\tilde{f}(\lambda)$ are used.

A basis $\{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n\}$ of F_{2^n} over F_2 is said to be a *trace orthonormal basis* if

$$tr_1^n(\alpha_i\alpha_j) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{otherwise.} \end{cases}$$

It is known that there exists a trace orthonormal basis of F_{2^n} over F_2 [13].

If we choose the basis as a trace orthonormal basis, then we have the relation

$$\begin{aligned} tr_1^n(\lambda x) &= \sum_{i=1}^{n}\sum_{j=1}^{n} \lambda_i x_j tr_1^n(\alpha_i\alpha_j) \\ &= \underline{\lambda} \cdot \underline{x}^{\mathrm{T}}. \end{aligned}$$

Using the trace orthonormal basis, it is easy to derive that the trace transform of $f(x)$ is equivalent to the Fourier transform of the corresponding Boolean function $f(\underline{x})$, that is,

$$F(\underline{\lambda}) = \hat{F}(\lambda).$$

Thus, if the trace transform of $f(x)$ only takes on the values $+1$ or -1, the corresponding Boolean function $f(\underline{x})$ becomes a bent function. Here, a function $f(x)$ defined on F_{2^n} is called a bent function if the trace transform of $f(x)$ only takes on the values $+1$ or -1.

In general, it is very difficult to classify the bent functions. Several different classes of bent functions on V_2^n are found for $n = 2m$, such as class M, class PS (PS− and PS+), class D, class C, and normal bent functions by Dobbertin, but they don't include all the known bent functions.

Firstly, a class M bent function is defined as [12]

$$f(\underline{x}_1, \underline{x}_2) = \underline{x}_1 \cdot \pi(\underline{x}_2)^{\mathrm{T}} + h(\underline{x}_2) \tag{2}$$

where $\underline{x}_1, \underline{x}_2 \in V_2^m$ and $\pi(\cdot)$ is any permutation on the m-dimensional binary vector space V_2^m and $h(\cdot)$ is any Boolean function on V_2^m.

The second class of bent functions introduced by Dillon [4] is class PS, which includes two classes of bent functions, termed PS− and PS+ as follows. Let $H_1, H_2, H_3, \cdots, H_{2^{m-1}}, H_{2^{m-1}+1}$ be m-dimensional subspaces of V_2^n satisfying

$$H_i \cap H_j = \{0\}, \quad \text{if } i \neq j.$$

Then the characteristic function of the set given by

$$D_- = \bigcup_{i=1}^{2^{m-1}} H_i^*$$

is called a class PS− bent function on V_2^n, where $H_i^* = H_i \backslash \{0\}$ and the characteristic function of the set given by

$$D_+ = \bigcup_{i=1}^{2^{m-1}+1} H_i$$

is called a class PS+ bent function on V_2^n.

Two other classes of bent functions are introduced by Carlet [2]. Let E be an m-dimensional subspace of V_2^n equal to $E_1 \times E_2$ and E_1 and E_2 be subspaces of V_2^m such that $dim E_1 + dim E_2 = m$. Let $\pi(\cdot)$ be any permutation on V_2^m such that $\pi(E_2) = E_1^{\perp}$, where $E_1^{\perp}$ is the dual space of E_1. Then the Boolean function defined by

$$f(\underline{x}_1, \underline{x}_2) = \underline{x}_1 \cdot \pi(\underline{x}_2)^{\mathrm{T}} + \phi_E(\underline{x}_1, \underline{x}_2) \tag{3}$$

is called a class D bent function, where the characteristic function $\phi_E(\underline{x}_1, \underline{x}_2)$ is defined as

$$\phi_E(\underline{x}_1, \underline{x}_2) = \begin{cases} 1, & \text{if } (\underline{x}_1, \underline{x}_2) \in E \\ 0, & \text{otherwise.} \end{cases}$$

Let $\pi(\cdot)$ be any permutation on V_2^m and L be any subspace of V_2^m such that, for any element λ of V_2^m, the set $\pi^{-1}(\lambda + L^{\perp})$ is a flat. Then the Boolean function defined by

$$f(\underline{x}_1, \underline{x}_2) = \underline{x}_1 \cdot \pi(\underline{x}_2)^{\mathrm{T}} + \phi_L(\underline{x}_1) \tag{4}$$

is called a class C bent function.

The last class of bent functions is normal bent functions by Dobbertin [5]. A Boolean function $f(\underline{x})$ defined on V_2^n is called *normal* if there is an affine subspace with dimension m, on which $f(\underline{x})$ is constant. He constructed a new class of normal bent functions using a mapping, called bent triple.

3. A New Class of Bent Functions

Let $m = ek$ for some positive integers e and k and E be the subset of F_{2^m} defined by

$$E = \{x \mid tr_e^m(x) = 0, x \in F_{2^m}\}. \tag{5}$$

From the balance property of the trace function $tr_e^m(x)$ from F_{2^m} to F_{2^e}, $|E| = 2^{m-e}$. Clearly, E is a linear subspace of F_{2^m}, because for any elements x, y in E, $x + y$ is also in E and 0 is in E. Using the trace orthonormal basis and the relation in (1), E can be considered as an $(m-e)$-dimensional subspace of V_2^m and then for any a in $F_{2^m} \backslash F_{2^e}$, $a+E$ is called an $(m-e)$-dimensional flat. It is clear that the characteristic function $\phi_E(x)$ of the subspace E in (5) can be obtained as

$$\phi_E(x) = [tr_e^m(x)]^{2^e-1} + 1. \tag{6}$$

The summation of the trace function over the flat $E' = a + E$ is given as in the following lemma.

Lemma 3: *Let $m = ek > 1$ for some positive integers e and k. Let E be the subspace of F_{2^m} in (5) and $E' = a + E$. Then for any element δ of F_{2^m}, we have*

$$\sum_{x\in E'}(-1)^{tr_1^m(\delta x)} = \begin{cases} (-1)^{tr_1^m(\delta a)}2^{m-e}, & \delta \in F_{2^e} \\ 0, & \delta \notin F_{2^e}. \end{cases} \tag{7}$$

Proof : Using the definition of E', the lefthand side of (7) can be written as

$$\begin{aligned}\sum_{x\in E'}(-1)^{tr_1^m(\delta x)} &= \sum_{x\in a+E}(-1)^{tr_1^m(\delta x)} \\ &= (-1)^{tr_1^m(\delta a)}\sum_{x\in E}(-1)^{tr_1^m(\delta x)}. \end{aligned} \tag{8}$$

If δ is in F_{2^e}, then for any $x \in E$, we have

$$\begin{aligned} tr_1^m(\delta x) &= tr_1^e(\delta tr_e^m(x)) \\ &= 0 \end{aligned}$$

and since $|E| = 2^{m-e}$, we have

$$\sum_{x\in E'}(-1)^{tr_1^m(\delta x)} = 2^{m-e}(-1)^{tr_1^m(\delta a)}.$$

If δ is not in F_{2^e}, the summation in (8) is rewritten as

$$\sum_{x\in E}(-1)^{tr_1^m(\delta x)} = 1 + \sum_{x\in E\backslash\{0\}}(-1)^{tr_1^m(\delta x)}. \tag{9}$$

Let α be a primitive element in F_{2^m} and $T = \frac{2^m-1}{2^e-1}$. Then $\beta = \alpha^T$ is a primitive element in F_{2^e}. Let $t = t_1T + t_2$, $0 \le t_1 \le 2^e - 2, 0 \le t_2 \le T - 1$. Then any nonzero element x in F_{2^m} can be written as

$$\begin{aligned} x &= \alpha^t \\ &= \alpha^{t_1T+t_2} \\ &= \beta^{t_1}\alpha^{t_2} \end{aligned}$$

and thus we have

$$\begin{aligned} tr_1^m(x) &= tr_1^m(\beta^{t_1}\alpha^{t_2}) \\ &= tr_1^e(\beta^{t_1}tr_e^m(\alpha^{t_2})). \end{aligned}$$

If x is in E, then for any integer i, $\beta^i x$ is also in E. Thus the set E defined in (5) can be written as

$$E = \{\beta^{t_1}\alpha^{t_2} \mid 0 \le t_1 \le 2^e - 2,\ t_2 \in I\} \cup \{0\}$$

where I is defined as

$$I = \{t_2 \mid tr_e^m(\alpha^{t_2}) = 0,\ 0 \le t_2 \le T - 1\}$$

and from the balance property of the trace function, the cardinality of I is given as

$$|I| = \frac{2^{m-e}-1}{2^e-1} = 2^{m-2e} + 2^{m-3e} + \cdots + 2^e + 1.$$

It is easy to prove that for any element δ of $F_{2^m}\backslash F_{2^e}$, $(tr_e^m(\delta x), tr_e^m(x)) = (0,0)$ occurs $2^{m-2e} - 1$ times as x varies over $F_{2^m}^* = F_{2^m}\backslash\{0\}$. This means that the cardinality of the subset I_δ of I defined by

$$I_\delta = \{t_2 \mid tr_e^m(\alpha^{t_2}\delta) = 0,\ t_2 \in I\}$$

is obtained as

$$|I_\delta| = \frac{2^{m-2e}-1}{2^e-1}$$

and then the cardinality of $I\backslash I_\delta$ is calculated as

$$|\ I\backslash I_\delta\ | = |I| - |I_\delta| = 2^{m-2e}.$$

For $x = \beta^{t_1}\alpha^{t_2}$ with a fixed t_2 in $I\backslash I_\delta$, the function $tr_e^m(\delta x)$ takes all elements in $\{\beta^0, \beta^1, \beta^2, \cdots, \beta^{2^e-2}\}$ exactly one time as t_1 varies over $0 \le t_1 \le 2^e - 2$. Thus we have

$$\sum_{t_1=0}^{2^e-2}(-1)^{tr_1^e(\beta^{t_1}tr_e^m(\delta\alpha^{t_2}))} = \begin{cases} 2^e - 1, & \text{if } t_2 \in I_\delta \\ -1, & \text{otherwise} \end{cases}$$

and equation (9) is written as

$$\begin{aligned}\sum_{x\in E}(-1)^{tr_1^m(\delta x)} &= 1 + \sum_{t_2\in I}\sum_{t_1=0}^{2^e-2}(-1)^{tr_1^e(\beta^{t_1}tr_e^m(\delta\alpha^{t_2}))} \\ &= 1 + (2^e - 1)\frac{2^{m-2e}-1}{2^e-1} + (-1)2^{m-2e} \\ &= 0. \end{aligned}$$

□

Let $n = 2m$ and x be an element in F_{2^n}. Let $V_{2^m}^2$ be the 2-dimensional vector space over F_{2^m}. Let (x_1, x_2) be an element in $V_{2^m}^2$, which is a vector representation of an element $x = x_1\alpha_1 + x_2\alpha_2$ in F_{2^n} by using a trace orthonormal basis $\{\alpha_1, \alpha_2\}$ of F_{2^n} over F_{2^m}. Then it is easy to derive that

$$tr_1^n(x\lambda) = tr_1^m(x_1\lambda_1 + x_2\lambda_2). \tag{10}$$

Using the above lemma, a new class of bent functions can be given as in the following theorem.

Theorem 4: *Let $n = 2m = 2ek$ for some positive integers e and k. Let E be the linear subspace of F_{2^m} defined in (5) and $\phi_E(x)$ be the characteristic function of E defined in (6). Let (x_1, x_2) be a vector representation of an element x in F_{2^n} by using a trace orthonormal basis of F_{2^n} over F_{2^m}. Let $\gamma \in F_{2^m}^*$ and $\gamma_i \in F_{2^m}$. Let $r = 2^{-c}(2^{ae} + 1)^{-1} \mod 2^m - 1$ such that $gcd(2^m - 1, 2^{ae} + 1) = 1$ and $s_i = r(2^{ie} + 1)$, where c and a are nonnegative integers, $0 \le a \le \lfloor\frac{k}{2}\rfloor$. Let $I = \{0, 1, 2, \cdots, \lfloor\frac{k}{2}\rfloor\}\backslash\{a\}$. Then the function defined on $V_{2^m}^2$*

$$\begin{aligned} f(x_1, x_2) &= tr_1^m(\gamma x_1 x_2^r) + \sum_{i\in I} tr_1^m(\gamma_i x_2^{s_i}) + \phi_E(x_1) \\ &= tr_1^m(\gamma x_1 x_2^r) \\ &\quad + \sum_{i\in I} tr_1^m(\gamma_i x_2^{s_i}) + [tr_e^m(x_1)]^{2^e-1} + 1 \end{aligned} \tag{11}$$

is a bent function and its trace transform defined on $V_{2^m}^2$ is given as

$$\begin{aligned}\tilde{f}(\lambda_1, \lambda_2) &= tr_1^m(\gamma^{-\frac{1}{r}}\lambda_1^{\frac{1}{r}}\lambda_2) + \sum_{i\in I} tr_1^m(\gamma_i\gamma^{-\frac{s_i}{r}}\lambda_1^{\frac{s_i}{r}}) \\ &\quad + [tr_e^m(B(\lambda_1, \lambda_2))]^{2^e-1} + 1 \end{aligned} \tag{12}$$

and it is also a bent function, where

$$\begin{aligned} &B(\lambda_1,\lambda_2)\\ &= \gamma^{-\frac{2^{-c}}{r}}(\lambda_1+\lambda_1^{2^{ae}})\lambda_2^{2^{-c}}+\gamma^{-\frac{2^{e-1-c}}{r}}\lambda_2^{2^{e-1-c}}\\ &\quad+\sum_{i\in I}(\gamma_i\gamma^{-\frac{s_i}{r}}(\lambda_1+\lambda_1^{2^{ie}})+\gamma_i^{2^{e-1}}\gamma^{-\frac{2^{e-1}\cdot s_i}{r}}). \end{aligned}$$

Proof : Using (10), the trace transform of $f(x_1,x_2)$ is given as

$$\begin{aligned} \hat{F}(\lambda_1,\lambda_2) &= (-1)^{\tilde{f}(\lambda_1,\lambda_2)}\\ &= \frac{1}{\sqrt{2^n}}\sum_{(x_1,x_2)\in V_{2^m}^2}(-1)^{f(x_1,x_2)+tr_1^m(\lambda_1x_1+\lambda_2x_2)}\\ &= \frac{1}{2^m}\sum_{x_2\in F_{2^m}}(-1)^{tr_1^m(\lambda_2x_2)+\sum_{i\in I}tr_1^m(\gamma_ix_2^{s_i})}\\ &\quad\cdot\sum_{x_1\in F_{2^m}}(-1)^{tr_1^m(\gamma x_1x_2^r)+[tr_e^m(x_1)]^{2^{e-1}}+1+tr_1^m(\lambda_1x_1)}\\ &= \frac{1}{2^m}\sum_{x_2\in F_{2^m}}(-1)^{tr_1^m(\lambda_2x_2)+\sum_{i\in I}tr_1^m(\gamma_ix_2^{s_i})}\\ &\quad\cdot\Bigg[\sum_{x_1\in F_{2^m}}(-1)^{tr_1^m(\gamma x_1x_2^r)+tr_1^m(\lambda_1x_1)}\\ &\quad-2\sum_{x_1\in E}(-1)^{tr_1^m(\gamma x_1x_2^r)+tr_1^m(\lambda_1x_1)}\Bigg]\\ &= \frac{1}{2^m}\sum_{x_2\in F_{2^m}}(-1)^{tr_1^m(\lambda_2x_2)+\sum_{i\in I}tr_1^m(\gamma_ix_2^{s_i})}\\ &\quad\cdot\Bigg[\sum_{x_1\in F_{2^m}}(-1)^{tr_1^m((\gamma x_2^r+\lambda_1)x_1)}\\ &\quad-2\sum_{x_1\in E}(-1)^{tr_1^m((\gamma x_2^r+\lambda_1)x_1)}\Bigg]\\ &= \frac{1}{2^m}\sum_{x_2\in F_{2^m}}(-1)^{tr_1^m(\lambda_2x_2)+\sum_{i\in I}tr_1^m(\gamma_ix_2^{s_i})}\\ &\quad\times\sum_{x_1\in F_{2^m}}(-1)^{tr_1^m((\gamma x_2^r+\lambda_1)x_1)}\\ &\quad-\frac{2}{2^m}\sum_{x_2\in F_{2^m}}(-1)^{tr_1^m(\lambda_2x_2)+\sum_{i\in I}tr_1^m(\gamma_ix_2^{s_i})}\\ &\quad\times\sum_{x_1\in E}(-1)^{tr_1^m((\gamma x_2^r+\lambda_1)x_1)}. \end{aligned} \tag{13}$$

From the character sum property [2], we have

$$\sum_{x_1\in F_{2^m}}(-1)^{tr_1^m((\gamma x_2^r+\lambda_1)x_1)} = \begin{cases} 2^m, & \text{if } x_2=\gamma^{-\frac{1}{r}}\lambda_1^{\frac{1}{r}}\\ 0, & \text{otherwise}\end{cases}$$

and thus the first term of (13) is rewritten as

$$(-1)^{tr_1^m(\lambda_2\gamma^{-\frac{1}{r}}\lambda_1^{\frac{1}{r}})+\sum_{i\in I}tr_1^m(\gamma_i\gamma^{-\frac{s_i}{r}}\lambda_1^{\frac{s_i}{r}})}. \tag{14}$$

From Lemma 3, we have

$$\sum_{x_1\in E}(-1)^{tr_1^m((\gamma x_2^r+\lambda_1)x_1)} = \begin{cases} 2^{m-e}, & \text{if } \gamma x_2^r+\lambda_1\in F_{2^e}\\ 0, & \text{otherwise}\end{cases}$$

and thus the second term of (13) is rewritten as

$$\begin{aligned} &\frac{2}{2^m}2^{m-e}\sum_{\gamma x_2^r+\lambda_1\in F_{2^e}}(-1)^{tr_1^m(\lambda_2x_2)+\sum_{i\in I}tr_1^m(\gamma_ix_2^{s_i})}\\ &\quad=\frac{2}{2^e}\sum_{x_2\in F_{2^e}}(-1)^{\{tr_1^m(\lambda_2\gamma^{-\frac{1}{r}}(x_2+\lambda_1)^{\frac{1}{r}})+\sum_{i\in I}tr_1^m(\gamma_i\gamma^{-\frac{s_i}{r}}(x_2+\lambda_1)^{\frac{s_i}{r}})\}}. \end{aligned} \tag{15}$$

From the definition of r and s_i and using $x_2^{2^e}=x_2$ and $x_2^{2^{ae}+1}=x_2^{2^{ie}+1}=x_2^2$ for $x_2\in F_{2^e}$, the exponent of (-1) in (15) is modified as

$$\begin{aligned} &tr_1^m(\lambda_2\gamma^{-\frac{1}{r}}(x_2+\lambda_1)^{2^c(2^{ae}+1)})\\ &\quad+\sum_{i\in I}tr_1^m(\gamma_i\gamma^{-\frac{s_i}{r}}(x_2+\lambda_1)^{2^{ie}+1})\\ &=tr_1^m(\lambda_2\gamma^{-\frac{1}{r}}(\lambda_1^{2^{ae}+1}+(\lambda_1+\lambda_1^{2^{ae}})x_2+x_2^{(2^{ae}+1)})^{2^c})\\ &\quad+\sum_{i\in I}tr_1^m(\gamma_i\gamma^{-\frac{s_i}{r}}(\lambda_1^{2^{ie}+1}+(\lambda_1+\lambda_1^{2^{ie}})x_2+x_2^{2^{ie}+1}))\\ &=tr_1^m(\lambda_2\gamma^{-\frac{1}{r}}\lambda_1^{2^c(2^{ae}+1)})\\ &\quad+tr_1^m(\lambda_2\gamma^{-\frac{1}{r}}(\lambda_1+\lambda_1^{2^{ae}})^{2^c}x_2^{2^c}+\lambda_2^{2^{e-1}}\gamma^{-\frac{2^{e-1}}{r}}x_2^{2^c})\\ &\quad+\sum_{i\in I}tr_1^m(\gamma_i\gamma^{-\frac{s_i}{r}}\lambda_1^{2^{ie}+1})\\ &\quad+\sum_{i\in I}tr_1^m(\gamma_i\gamma^{-\frac{s_i}{r}}(\lambda_1+\lambda_1^{2^{ie}})x_2+\gamma_i^{2^{e-1}}\gamma^{-\frac{2^{e-1}s_i}{r}}x_2)\\ &=tr_1^m(\lambda_2\lambda_1^{\frac{1}{r}}\gamma^{-\frac{1}{r}})+\sum_{i\in I}tr_1^m(\gamma_i\gamma^{-\frac{s_i}{r}}\lambda_1^{\frac{s_i}{r}})\\ &\quad+tr_1^m([\lambda_2^{2^{-c}}\gamma^{-\frac{2^{-c}}{r}}(\lambda_1+\lambda_1^{2^{ae}})+\lambda_2^{2^{e-1-c}}\gamma^{-\frac{2^{e-1-c}}{r}}\\ &\quad+\sum_{i\in I}(\gamma_i\gamma^{-\frac{s_i}{r}}(\lambda_1+\lambda_1^{2^{ie}})+\gamma_i^{2^{e-1}}\gamma^{-\frac{2^{e-1}s_i}{r}})]x_2)\\ &=tr_1^m(\lambda_2\lambda_1^{\frac{1}{r}}\gamma^{-\frac{1}{r}})+\sum_{i\in I}tr_1^m(\gamma_i\gamma^{-\frac{s_i}{r}}\lambda_1^{\frac{s_i}{r}})\\ &\quad+tr_1^m(B(\lambda_1,\lambda_2)x_2) \end{aligned}$$

where

$$\begin{aligned} B(\lambda_1,\lambda_2) &= \lambda_2^{2^{-c}}\gamma^{-\frac{2^{-c}}{r}}(\lambda_1+\lambda_1^{2^{ae}})\\ &\quad+\lambda_2^{2^{e-1-c}}\gamma^{-\frac{2^{e-1-c}}{r}}\\ &\quad+\sum_{i\in I}(\gamma_i\gamma^{-\frac{s_i}{r}}(\lambda_1+\lambda_1^{2^{ie}})+\gamma_i^{2^{e-1}}\gamma^{-\frac{2^{e-1}s_i}{r}}). \end{aligned}$$

Then the second term of (13) is written as

$$\frac{2}{2^e}(-1)^{tr_1^m(\lambda_2\lambda_1^{\frac{1}{r}}\gamma^{-\frac{1}{r}})+\sum_{i\in I}tr_1^m(\gamma_i\gamma^{-\frac{s_i}{r}}\lambda_1^{\frac{s_i}{r}})} \times \sum_{x_2\in F_{2^e}}(-1)^{tr_1^m(B(\lambda_1,\lambda_2)x_2)} = \begin{cases} 2(-1)^{tr_1^m(\lambda_2\lambda_1^{\frac{1}{r}}\gamma^{-\frac{1}{r}})+\sum_{i\in I}tr_1^m(\gamma_i\gamma^{-\frac{s_i}{r}}\lambda_1^{\frac{s_i}{r}})}, \\ \qquad \text{if } tr_e^m(B(\lambda_1,\lambda_2))=0 \\ 0, \quad \text{otherwise.} \end{cases} \tag{16}$$

Plugging (14) and (16) into (13), we have

$$\hat{F}(\lambda_1,\lambda_2) = \begin{cases} -(-1)^{tr_1^m(\lambda_2\lambda_1^{\frac{1}{r}}\gamma^{-\frac{1}{r}})+\sum_{i\in I}tr_1^m(\gamma_i\gamma^{-\frac{s_i}{r}}\lambda_1^{\frac{s_i}{r}})}, \\ \qquad \text{if } tr_e^m(B(\lambda_1,\lambda_2))=0 \\ (-1)^{tr_1^m(\lambda_2\lambda_1^{\frac{1}{r}}\gamma^{-\frac{1}{r}})+\sum_{i\in I}tr_1^m(\gamma_i\gamma^{-\frac{s_i}{r}}\lambda_1^{\frac{s_i}{r}})}, \\ \qquad \text{otherwise.} \end{cases} \tag{17}$$

Therefore the function $f(x_1, x_2)$ on $V_{2^m}^2$ is a bent function. Using (17) and the relation

$$[tr_e^m(B(\lambda_1,\lambda_2))]^{2^e-1}+1 = \begin{cases} 1, & \text{if } tr_e^m(B(\lambda_1,\lambda_2))=0 \\ 0, & \text{otherwise,} \end{cases}$$

the trace transform $\tilde{f}(\lambda_1, \lambda_2)$ in (12) can be derived. □

The bent function in (11) belongs to a class M bent function defined in (2) if $\phi_E(x_1)$ is deleted. If the second term depending only on x_2 is deleted in (11), it belongs to a bent function of class C defined in (4), which was introduced by Carlet. It is clear that for a fixed $x_2 = c_0 \in F_{2^m}$, the bent function $f(x_1, c_0)$ in (11) is not a constant as x_1 varies over F_{2^m}. Therefore, it is different from the normal bent functions introduced by Dobbertin [5]. Two examples for the new bent functions derived in Theorem 4 are given as follows.

Example 5: *Let $n = 20$, $m = 10$, $e = 2$, and $k = 5$. Let (x_1, x_2) be a vector representation of an element x in $F_{2^{20}}$ by using a trace orthonormal basis $\{\alpha_1, \alpha_2\}$ of $F_{2^{20}}$ over $F_{2^{10}}$. Let E be the subspace of $F_{2^{10}}$ given by*

$$E = \{x_1 |\, tr_2^{10}(x_1) = 0, x_1 \in F_{2^{10}}\}.$$

a) *Let $\gamma \in F_{2^{10}}^*$ and $\gamma_0, \gamma_2 \in F_{2^{10}}$. Let $\frac{1}{r} = 2^2 + 1$, where $r = 614$, $a = 1$, and $c = 0$. The index set I is $\{0, 1, 2\}\backslash\{1\}$ and $s_0 = 614\times 2 = 205$ and $s_2 = 614\times(2^4+1) = 208$. Then the function defined on $V_{2^{10}}^2$*

$$f(x_1,x_2) = tr_1^{10}(\gamma x_1 x_2^{614}) + tr_1^{10}(\gamma_0 x_2^{205} + \gamma_2 x_2^{208}) + [tr_2^{10}(x_1)]^{2^2-1}+1$$

is a bent function and its trace transform defined on $V_{2^{10}}^2$ is expressed as

$$\tilde{f}(\lambda_1,\lambda_2) = tr_1^{10}(\gamma^{-5}\lambda_1^5\lambda_2) + tr_1^{10}(\gamma_0\gamma^{-2}\lambda_1^2 + \gamma_2\gamma^{-17}\lambda_1^{17}) + [tr_2^{10}(B(\lambda_1,\lambda_2))]^{2^2-1}+1$$

where

$$B(\lambda_1,\lambda_2) = \gamma^{-5}(\lambda_1+\lambda_1^{2^2})\lambda_2 + \gamma^{-10}\lambda_2^2 + (\gamma_0^2\gamma^{-4} + \gamma_2\gamma^{-17}(\lambda_1+\lambda_1^{2^4}) + \gamma_2^2\gamma^{-34}).$$

b) *Let $\gamma \in F_{2^{10}}^*$ and $\gamma_1, \gamma_2 \in F_{2^{10}}$. Let $r = 1$, where $a = 0$ and $c = m-1$. Let $s_1 = 2^2+1 = 5$ and $s_2 = 2^4+1 = 17$. Then the function defined on $V_{2^{10}}^2$*

$$f(x_1,x_2) = tr_1^{10}(\gamma x_1 x_2) + tr_1^{10}(\gamma_1 x_2^5 + \gamma_2 x_2^{17}) + [tr_2^{10}(x_1)]^{2^2-1}+1$$

is a bent function and its trace transform defined on $V_{2^{10}}^2$ is given as

$$\tilde{f}(\lambda_1,\lambda_2) = tr_1^{10}(\gamma^{-1}\lambda_1\lambda_2) + tr_1^{10}(\gamma_1\gamma^{-5}\lambda_1^5 + \gamma_2\gamma^{-17}\lambda_1^{17}) + [tr_2^{10}(B(\lambda_1,\lambda_2))]^{2^2-1}+1$$

where

$$B(\lambda_1,\lambda_2) = \gamma^{-2^2}\lambda_2^{2^2} + (\gamma_1\gamma^{-5}(\lambda_1+\lambda_1^{2^2}) + \gamma_1^2\gamma^{-10}) + (\gamma_2\gamma^{-17}(\lambda_1+\lambda_1^{2^4}) + \gamma_2^2\gamma^{-34}).$$

□

4. Class D-Type Generalized Bent Functions

Let q be a positive integer and V_q^n be the n-dimensional vector space over the set of integers modulo q, J_q. Let $\omega = e^{j\frac{2\pi}{q}}$, $j = \sqrt{-1}$. Let $f(\underline{x})$ be a function from V_q^n to J_q. The Fourier transform of $f(\underline{x})$ is defined as

$$F(\underline{\lambda}) = \frac{1}{\sqrt{q^n}}\sum_{\underline{x}\in V_q^n}\omega^{f(\underline{x})-\underline{\lambda}\cdot\underline{x}^{\mathrm{T}}}, \quad \text{all } \underline{\lambda}\in V_q^n.$$

Then a generalized bent function is defined as:

Definition 6: *[Kumar, Scholtz, and Welch [7]] : A function $f(\underline{x})$ from V_q^n to J_q is said to be a generalized bent function if the Fourier coefficients $F(\underline{\lambda})$ of $f(\underline{x})$ only take the values of unit magnitude for any $\underline{\lambda} \in V_q^n$.* □

A generalized bent function is called a *regular bent function*, if its Fourier coefficients are integral powers of ω, *i.e.*,

$$F(\underline{\lambda}) = \omega^{\tilde{f}(\underline{\lambda})}, \quad \text{all } \underline{\lambda}\in V_q^n$$

where $\tilde{f}(\underline{\lambda}) \in J_q$. It is clear that for a regular bent function $f(\underline{x})$, its Fourier transform $\tilde{f}(\underline{\lambda})$ is also a generalized bent function from V_q^n to J_q.

In this section, we assume that the integer q is an odd prime p and we generalized the class D bent functions defined in (3) into p-ary generalized bent functions from $V_{p^m}^2$ to F_p, where $V_{p^m}^2$ is the 2-dimensional vector space over the finite field F_{p^m} with p^m elements. Let $f(x_1, x_2)$ be a function from $V_{p^m}^2$ to F_p. Kumar, Scholtz, and Welch introduced trace transform for a function from F_{2^n} to F_2 [7], which can be generalized as follows:

Definition 7: *Let $f(x_1, x_2)$ be a function from $V_{p^m}^2$ to F_p. Then the trace transform of $f(x_1, x_2)$ and its inverse trace transform are defined as*

$$\hat{F}(\lambda_1, \lambda_2) = \frac{1}{p^m} \sum_{(x_1,x_2)\in V_{p^m}^2} \omega^{f(x_1,x_2)-tr_1^m(\lambda_1 x_1+\lambda_2 x_2)}, \quad \text{all } (\lambda_1, \lambda_2) \in V_{p^m}^2$$

$$\omega^{f(x_1,x_2)} = \frac{1}{p^m} \sum_{(\lambda_1,\lambda_2)\in V_{p^m}^2} \hat{F}(\lambda_1, \lambda_2)\omega^{tr_1^m(\lambda_1 x_1+\lambda_2 x_2)}, \quad \text{all } (x_1, x_2) \in V_{p^m}^2.$$

□

In a similar way to the binary case, the elements x_1, x_2, λ_1, and λ_2 in F_{p^m} can be related to the elements $\underline{x}_1, \underline{x}_2, \underline{\lambda}_1$, and $\underline{\lambda}_2$ in the m-dimensional vector space over F_p, V_p^m by

$$x_j = \sum_{i=1}^{m} x_{ji}\alpha_i \Rightarrow \underline{x}_j = (x_{j1}, x_{j2}, x_{j3}, \cdots, x_{jm}) \tag{18}$$

$$\lambda_j = \sum_{i=1}^{m} \lambda_{ji}\alpha_i \Rightarrow \underline{\lambda}_j = (\lambda_{j1}, \lambda_{j2}, \lambda_{j3}, \cdots, \lambda_{jm}) \tag{19}$$

where $j = 1, 2$, x_{ji} and λ_{ji} are in F_p and $\{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_m\}$ is some basis of F_{p^m} over F_p. By replacing x_1 and x_2 in F_{p^m} by $\underline{x}_1$ and $\underline{x}_2$ in V_p^m, a function $f(x_1, x_2)$ from $V_{p^m}^2$ to F_p becomes the corresponding function $f(\underline{x}_1, \underline{x}_2)$ from V_p^{2m} to F_p.

A basis $\{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_m\}$ of F_{p^m} over F_p is said to be a trace orthogonal basis if

$$tr_1^m(\alpha_i\alpha_j) = \begin{cases} u_i, & \text{if } i = j \\ 0, & \text{otherwise} \end{cases}$$

where u_i is in F_p^*. It is known that for any positive integer m and an odd prime p, there exists a trace orthogonal basis of F_{p^m} over F_p [13].

If we choose the basis as a trace orthogonal basis, then we have the relations

$$tr_1^m(\lambda_1 x_1) = \sum_{i=1}^{m}\sum_{j=1}^{m} \lambda_{1i}x_{1j}tr_1^m(\alpha_i\alpha_j) = \sum_{i=1}^{m} u_i\lambda_{1i}x_{1i} \tag{20}$$

and

$$tr_1^m(\lambda_2 x_2) = \sum_{i=1}^{m}\sum_{j=1}^{m} \lambda_{2i}x_{2j}tr_1^m(\alpha_i\alpha_j) = \sum_{i=1}^{m} u_i\lambda_{2i}x_{2i}. \tag{21}$$

Let $\lambda_{ji}' = u_i\lambda_{ji}$ for $j = 1, 2$ and i, $1 \le i \le m$ and $\underline{\lambda}_j' = (\lambda_{j1}', \lambda_{j2}', \cdots, \lambda_{jm}')$. Using the relations in (20) and (21), we have

$$tr_1^m(\lambda_1 x_1 + \lambda_2 x_2) = \sum_{i=1}^{m} \lambda_{1i}'x_{1i} + \lambda_{2i}'x_{2i} = (\underline{\lambda}_1', \underline{\lambda}_2') \cdot (\underline{x}_1, \underline{x}_2)^{\mathrm{T}}.$$

Then the trace transform of the function $f(x_1, x_2)$ from $V_{p^m}^2$ to F_p can be obtained from the Fourier transform of the corresponding function $f(\underline{x}_1, \underline{x}_2)$ from V_p^{2m} to F_p by the relation

$$\hat{F}(\lambda_1, \lambda_2) = F(\underline{\lambda}_1', \underline{\lambda}_2').$$

Thus, the set of the trace transform values of $f(x_1, x_2)$ is the same as that of the Fourier transform values of $f(\underline{x}_1, \underline{x}_2)$. Therefore if the trace transform of $f(x_1, x_2)$ only takes the values of unit magnitude, the corresponding function $f(\underline{x}_1, \underline{x}_2)$ becomes a generalized bent function. Now a function $f(x_1, x_2)$ defined on $V_{p^m}^2$ is called a generalized bent function if the trace transform of $f(x_1, x_2)$ only takes the value of unit magnitude.

In this section, it is only considered the regular bent function given by

$$\hat{F}(\lambda_1, \lambda_2) = \omega^{\tilde{f}(\lambda_1,\lambda_2)}$$

and when we say the trace transform of $f(x_1, x_2)$, it means $\tilde{f}(\lambda_1, \lambda_2)$ or $\hat{F}(\lambda_1, \lambda_2)$.

Similarly to the binary case [2], we have the following lemma for a function defined on $V_{p^m}^2$.

Lemma 8: *Let p be an odd prime and $\omega = e^{j\frac{2\pi}{p}}$. Let E be a linear subspace of $V_{p^m}^2$ and $E^\perp$ be the linear subspace of $V_{p^m}^2$ satisfying $tr_1^m(\underline{x} \cdot \underline{y}^{\mathrm{T}}) = 0$ for any $\underline{x} = (x_1, x_2) \in E$ and $\underline{y} = (y_1, y_2) \in E^\perp$. Let $f(\underline{x})$ be a generalized regular bent function from $V_{p^m}^2$ to F_p and $\tilde{f}(\underline{x})$ be the trace transform of $f(\underline{x})$. Then for any two elements $\underline{c} = (c_1, c_2)$ and $\underline{d} = (d_1, d_2)$ in $V_{p^m}^2$, we have*

$$\sum_{\underline{x}\in\underline{c}+E} \omega^{f(\underline{x})-tr_1^m(\underline{d}\cdot\underline{x}^{\mathrm{T}})} = p^{dimE-m}\omega^{-tr_1^m(\underline{c}\cdot\underline{d}^{\mathrm{T}})} \sum_{\underline{x}\in\underline{d}+E^\perp} \omega^{\tilde{f}(\underline{x})+tr_1^m(\underline{c}\cdot\underline{x}^{\mathrm{T}})}. \tag{22}$$

If $dimE = m$ and the restriction of $f(\underline{x})$ to E is some constant s in F_p, then the restriction of $\tilde{f}(\underline{x})$ to $E^\perp$ is also s.

Proof : Using the definition of trace transform, the summation of the righthand side of (22) is written as

$$\sum_{\underline{x}\in d+E^\perp} \omega^{\tilde{f}(\underline{x})+tr_1^m(\underline{c}\cdot\underline{x}^{\mathrm{T}})} = \frac{1}{p^m} \sum_{\underline{x}\in\underline{d}+E^\perp} \sum_{\underline{y}\in V_{p^m}^2} \omega^{f(\underline{y})-tr_1^m(\underline{y}\cdot\underline{x}^{\mathrm{T}})+tr_1^m(\underline{c}\cdot\underline{x}^{\mathrm{T}})} = \frac{1}{p^m} \sum_{\underline{y}\in V_{p^m}^2} \omega^{f(\underline{y})} \sum_{\underline{x}\in\underline{d}+E^\perp} \omega^{-tr_1^m((\underline{y}-\underline{c})\cdot\underline{x}^{\mathrm{T}})}.$$

Using a trace orthogonal basis of F_{p^m} over F_p, (18), (19), (20), and (21), the inner summation is computed as

$$\begin{aligned}
&\sum_{\underline{x}\in\underline{d}+E^\perp} \omega^{-tr_1^m((\underline{y}-\underline{c})\cdot\underline{x}^{\mathrm{T}})} \\
&= \omega^{-tr_1^m((\underline{y}-\underline{c})\cdot\underline{d}^{\mathrm{T}})} \sum_{\underline{x}\in E^\perp} \omega^{-tr_1^m((\underline{y}-\underline{c})\cdot\underline{x}^{\mathrm{T}})} \\
&= \omega^{-tr_1^m((\underline{y}-\underline{c})\cdot\underline{d}^{\mathrm{T}})} \sum_{(\underline{x}_1,\underline{x}_2)\in E^\perp} \omega^{-\sum_{i=1}^m u_i[(y_{1i}-c_{1i})x_{1i}+(y_{2i}-c_{2i})x_{2i}]} \\
&= \begin{cases} |E^\perp|\omega^{-tr_1^m((\underline{y}-\underline{c})\cdot\underline{d}^{\mathrm{T}})}, & \text{if } \underline{y}-\underline{c}\in E \\ 0, & \text{otherwise} \end{cases} \qquad (23)
\end{aligned}$$

where $|E^\perp| = p^{2m-dimE}$ and we abuse the notation $E^\perp$ as the set of the $2m$-tuple vectors corresponding to the elements in $E^\perp$. Thus we have

$$\begin{aligned}
&\sum_{\underline{x}\in\underline{d}+E^\perp} \omega^{\tilde{f}(\underline{x})+tr_1^m(\underline{c}\cdot\underline{x}^{\mathrm{T}})} \\
&= p^{m-dimE}\omega^{tr_1^m(\underline{c}\cdot\underline{d}^{\mathrm{T}})} \sum_{\underline{y}\in\underline{c}+E} \omega^{f(\underline{y})-tr_1^m(\underline{d}\cdot\underline{y}^{\mathrm{T}})}.
\end{aligned}$$

Thus we proved the first part of the lemma.

Assume that E has dimension m and $\underline{c} = \underline{d} = \underline{0}$ and thus $E^\perp$ has dimension m. Then equation (22) reduces to

$$\sum_{\underline{x}\in E} \omega^{f(\underline{x})} = \sum_{\underline{x}\in E^\perp} \omega^{\tilde{f}(\underline{x})}.$$

If the restriction of $f(\underline{x})$ to E is some constant s in F_p, then the lefthand side of the above equation becomes $p^m\omega^s$ and thus in the righthand side, the restriction of $\tilde{f}(\underline{x})$ to $E^\perp$ must be s. □

Let E and $E^\perp$ be a linear subspace of $V_{p^m}^2$ and its dual space satisfying $tr_1^m(\underline{x}\cdot\underline{\lambda}^{\mathrm{T}}) = 0$ for any $\underline{x}\in E$ and $\underline{\lambda}\in E^\perp$, respectively. Then their characteristic functions $\phi_E(\underline{x})$ and $\phi_{E^\perp}(\underline{\lambda})$ are defined as

$$\phi_E(\underline{x}) = \begin{cases} b, & \underline{x}\in E \\ 0, & \underline{x}\notin E \end{cases} \qquad (24)$$

$$\phi_{E^\perp}(\underline{\lambda}) = \begin{cases} b, & \underline{\lambda}\in E^\perp \\ 0, & \underline{\lambda}\notin E^\perp \end{cases} \qquad (25)$$

where b is some element in F_p^*.

Using the previous lemma, new generalized bent functions can be constructed as in the following theorem.

Theorem 9: *Let E and $E^\perp$ be an m-dimensional linear subspace of $V_{p^m}^2$ and its dual space satisfying $tr_1^m(\underline{x}\cdot\underline{\lambda}^{\mathrm{T}}) = 0$ for any $\underline{x}\in E$ and $\underline{\lambda}\in E^\perp$, respectively. Let $\phi_E(\underline{x})$ and $\phi_{E^\perp}(\underline{\lambda})$ be the characteristic functions of E and $E^\perp$ defined in (24) and (25), respectively. Let $f(\underline{x})$ be a generalized regular bent function from $V_{p^m}^2$ to F_p whose restriction to E is affine, i.e., $tr_1^m(\underline{a}\cdot\underline{x}^{\mathrm{T}})+\epsilon, \underline{a}\in V_{p^m}^2, \epsilon\in F_p$. Let $\tilde{f}(\underline{\lambda})$ be the trace transform of $f(\underline{x})$. Then the function on $V_{p^m}^2$ defined by*

$$f(\underline{x}) + \phi_E(\underline{x})$$

is a generalized regular bent function and its trace transform is given as

$$\tilde{f}(\underline{\lambda}) + \phi_{E^\perp}(\underline{\lambda}-\underline{a}).$$

Proof : Using the definition of the trace transform of $f(\underline{x}) + \phi_E(\underline{x})$, we have

$$\begin{aligned}
&\sum_{\underline{x}\in V_{p^m}^2} \omega^{f(\underline{x})+\phi_E(\underline{x})-tr_1^m(\underline{\lambda}\cdot\underline{x}^{\mathrm{T}})} \\
&= \sum_{\underline{x}\in V_{p^m}^2\setminus E} \omega^{f(\underline{x})-tr_1^m(\underline{\lambda}\cdot\underline{x}^{\mathrm{T}})} + \omega^b \sum_{\underline{x}\in E} \omega^{f(\underline{x})-tr_1^m(\underline{\lambda}\cdot\underline{x}^{\mathrm{T}})} \\
&= \sum_{\underline{x}\in V_{p^m}^2} \omega^{f(\underline{x})-tr_1^m(\underline{\lambda}\cdot\underline{x}^{\mathrm{T}})} \\
&\quad -(1-\omega^b)\sum_{\underline{x}\in E} \omega^{f(\underline{x})-tr_1^m(\underline{\lambda}\cdot\underline{x}^{\mathrm{T}})}. \qquad (26)
\end{aligned}$$

From the definition of the trace transform of $f(\underline{x})$, the first term in (26) is given as

$$\sum_{\underline{x}\in V_{p^m}^2} \omega^{f(\underline{x})-tr_1^m(\underline{\lambda}\cdot\underline{x}^{\mathrm{T}})} = p^m\omega^{\tilde{f}(\underline{\lambda})}.$$

Let $\underline{c} = \underline{0}$, $\underline{d} = \underline{\lambda}$, and $dimE = m$ in (22). Then we have

$$\sum_{\underline{x}\in E} \omega^{f(\underline{x})-tr_1^m(\underline{\lambda}\cdot\underline{x}^{\mathrm{T}})} = \sum_{\underline{x}\in\underline{\lambda}+E^\perp} \omega^{\tilde{f}(\underline{x})}. \qquad (27)$$

Similarly to (23) and using that the restriction of $f(\underline{x})$ to E is $tr_1^m(\underline{a}\cdot\underline{x}^{\mathrm{T}})+\epsilon$, the lefthand side of (27) can be computed as

$$\begin{aligned}
&\sum_{\underline{x}\in E} \omega^{f(\underline{x})-tr_1^m(\underline{\lambda}\cdot\underline{x}^{\mathrm{T}})} \\
&= \sum_{\underline{x}\in E} \omega^{tr_1^m(\underline{a}\cdot\underline{x}^{\mathrm{T}})+\epsilon-tr_1^m(\underline{\lambda}\cdot\underline{x}^{\mathrm{T}})} \\
&= \omega^\epsilon \sum_{\underline{x}\in E} \omega^{-tr_1^m((\underline{\lambda}-\underline{a})\cdot\underline{x}^{\mathrm{T}})} \\
&= \begin{cases} p^m\omega^\epsilon, & \text{if } \underline{\lambda}-\underline{a}\in E^\perp \\ 0, & \text{if } \underline{\lambda}-\underline{a}\notin E^\perp. \end{cases} \qquad (28)
\end{aligned}$$

Thus if $\underline{\lambda}-\underline{a}\notin E^\perp$, equation (26) reduces to

$$\sum_{\underline{x}\in V_{p^m}^2} \omega^{f(\underline{x})+\phi_E(\underline{x})-tr_1^m(\underline{\lambda}\cdot\underline{x}^{\mathrm{T}})} = p^m\omega^{\tilde{f}(\underline{\lambda})}. \qquad (29)$$

If $\underline{\lambda}-\underline{a}\in E^\perp$, equation (27) becomes

$$\sum_{\underline{x}\in\underline{\lambda}+E^\perp} \omega^{\tilde{f}(\underline{x})} = p^m\omega^\epsilon$$

and then we have

$$\omega^{\tilde{f}(\underline{x})} = \omega^\epsilon, \quad \text{for } \underline{x}\in\underline{\lambda}+E^\perp. \qquad (30)$$

It is clear that $\underline{x}\in\underline{\lambda}+E^\perp$ is equivalent to $\underline{x}\in\underline{a}+E^\perp$ because $\underline{\lambda}+E^\perp = \underline{a}+E^\perp+E^\perp = \underline{a}+E^\perp$. Thus equation (30) is

rewritten as

$$\omega^{\tilde{f}(\underline{x})} = \omega^{\epsilon}, \quad \text{for } \underline{x} \in \underline{a} + E^{\perp}. \tag{31}$$

Replacing the dummy variable $\underline{x}$ by $\underline{\lambda}$, equation (31) can be given as

$$\omega^{\tilde{f}(\underline{\lambda})} = \omega^{\epsilon}, \quad \text{for } \underline{\lambda} \in \underline{a} + E^{\perp}. \tag{32}$$

Therefore, equation (26) is derived as

$$\begin{aligned} &\sum_{\underline{x} \in V_{p^m}^2} \omega^{f(\underline{x}) + \phi_E(\underline{x}) - tr_1^m(\underline{\lambda} \cdot \underline{x}^{\mathrm{T}})} \\ &\quad = p^m \omega^{\tilde{f}(\underline{\lambda})} - (1 - \omega^b) p^m \omega^{\tilde{f}(\underline{\lambda})} \\ &\quad = p^m \omega^{\tilde{f}(\underline{\lambda}) + b}, \quad \text{for } \underline{\lambda} - \underline{a} \in E^{\perp}. \end{aligned} \tag{33}$$

From (29) and (33), we have

$$\sum_{\underline{x} \in V_{p^m}^2} \omega^{f(\underline{x}) + \phi_E(\underline{x}) - tr_1^m(\underline{\lambda} \cdot \underline{x}^{\mathrm{T}})} = p^m \omega^{\tilde{f}(\underline{\lambda}) + \phi_{E^{\perp}}(\underline{\lambda} - \underline{a})}.$$

Thus the trace transform of $f(\underline{x}) + \phi_E(\underline{x})$ is obtained as

$$\frac{1}{p^m} \sum_{\underline{x} \in V_{p^m}^2} \omega^{f(\underline{x}) + \phi_E(\underline{x}) - tr_1^m(\underline{\lambda} \cdot \underline{x}^{\mathrm{T}})} = \omega^{\tilde{f}(\underline{\lambda}) + \phi_{E^{\perp}}(\underline{\lambda} - \underline{a})}.$$

Therefore $f(\underline{x})$ is a generalized regular bent function and its trace transform is given as

$$\tilde{f}(\underline{\lambda}) + \phi_{E^{\perp}}(\underline{\lambda} - \underline{a}). \qquad \square$$

It is easy to find an m-dimensional linear subspace E of $V_{p^m}^2$ and its dual space $E^{\perp}$ satisfying $tr_1^m(\underline{x} \cdot \underline{\lambda}^{\mathrm{T}}) = 0$ for any $\underline{x} \in E$ and $\underline{\lambda} \in E^{\perp}$ as follows:

$$\begin{aligned} E &= \{(0, \beta) \mid \beta \in F_{p^m}\} \\ E^{\perp} &= \{(\beta, 0) \mid \beta \in F_{p^m}\} \end{aligned}$$

or for any $\delta \in F_{p^m}^*$, the m-dimensional linear subspaces E and $E^{\perp}$ can also be given as

$$E = \{(\delta x_2, x_2) \mid x_2 \in F_{p^m}\} \tag{34}$$

$$E^{\perp} = \{(-\delta^{-1}\lambda_2, \lambda_2) \mid \lambda_2 \in F_{p^m}\}. \tag{35}$$

Using (24) and (25), the characteristic functions of the linear subspaces E and $E^{\perp}$ given in (34) and (35) can be expressed as

$$\phi_E(x_1, x_2) = (p - b)[\delta^{-1} x_1 - x_2]^{p^m - 1} + b \tag{36}$$

$$\phi_{E^{\perp}}(\lambda_1, \lambda_2) = (p - b)[\delta \lambda_1 + \lambda_2]^{p^m - 1} + b \tag{37}$$

where b is some element in F_p^*.

Let $\gamma \in F_{p^m}^*$, $\epsilon \in F_p$, and $gcd(r, p^m - 1) = 1$. Then a class M-type generalized bent function can be represented as

$$f(x_1, x_2) = tr_1^m(\gamma x_1 x_2^r) + tr_1^m(g(x_2)) + \epsilon$$

where $g(x_2)$ is a function defined on F_{p^m}. A class M-type generalized bent function whose restriction to the subspace E in (34) is affine (that is, ϵ) is expressed as follows:

$$f(x_1, x_2) = tr_1^m(\gamma x_1 x_2^r) - tr_1^m(\gamma \delta x_2^{r+1}) + \epsilon. \tag{38}$$

It can be easily proved that if (x_1, x_2) is in E, then $x_1 = \delta x_2$ from (34) and putting $x_1 = \delta x_2$ into (38), we have $f(\delta x_2, x_2) = \epsilon$. The trace transform of $f(x_1, x_2)$ is obtained as

$$\begin{aligned} &\hat{F}(\lambda_1, \lambda_2) \\ &\quad = \frac{1}{p^m} \sum_{(x_1, x_2) \in V_{p^m}^2} \omega^{\{tr_1^m(\gamma x_1 x_2^r) - tr_1^m(\gamma \delta x_2^{r+1}) + \epsilon - tr_1^m(\lambda_1 x_1 + \lambda_2 x_2)\}} \\ &\quad = \frac{1}{p^m} \sum_{x_2 \in F_{p^m}} \omega^{-tr_1^m(\gamma \delta x_2^{r+1}) - tr_1^m(\lambda_2 x_2) + \epsilon} \\ &\qquad \times \sum_{x_1 \in F_{p^m}} \omega^{tr_1^m((\gamma x_2^r - \lambda_1) x_1)} \\ &\quad = \omega^{-tr_1^m(\gamma^{-\frac{1}{r}} \lambda_1^{\frac{1}{r}} \lambda_2) - tr_1^m(\gamma^{-\frac{1}{r}} \delta \lambda_1^{\frac{r+1}{r}}) + \epsilon}. \end{aligned}$$

Thus, we have

$$\begin{aligned} \tilde{f}(\lambda_1, \lambda_2) = &-tr_1^m(\gamma^{-\frac{1}{r}} \lambda_1^{\frac{1}{r}} \lambda_2) \\ &-tr_1^m(\gamma^{-\frac{1}{r}} \delta \lambda_1^{\frac{r+1}{r}}) + \epsilon. \end{aligned} \tag{39}$$

By putting $\lambda_1 = -\delta^{-1}\lambda_2$ into (39), it is easy to check that the restriction of $\tilde{f}(\lambda_1, \lambda_2)$ to $E^{\perp}$ defined in (35) is also affine, that is, ϵ.

Using (36), (37), Theorem 9, and the class M-type generalized bent function defined in (38), a new class of D-type generalized bent function is constructed as in the following theorem.

Theorem 10: *Let E and $E^{\perp}$ be the linear subspace of $V_{p^m}^2$ defined in (34) and its dual space defined in (35), respectively. Let $\phi_E(x_1, x_2)$ and $\phi_{E^{\perp}}(\lambda_1, \lambda_2)$ be the characteristic functions of E and $E^{\perp}$ defined in (36) and (37), respectively. Let $f(x_1, x_2)$ be the M-type generalized bent function defined in (38). Then the function defined by*

$$\begin{aligned} &f(x_1, x_2) + \phi_E(x_1, x_2) \\ &\quad = tr_1^m(\gamma x_1 x_2^r) - tr_1^m(\gamma \delta x_2^{r+1}) + \epsilon \\ &\qquad + (p - b)[\delta^{-1} x_1 - x_2]^{p^m - 1} + b \end{aligned}$$

is a generalized regular bent function, termed class D-type generalized bent function. And its trace transform is also the generalized regular bent function given by

$$\begin{aligned} &\tilde{f}(\lambda_1, \lambda_2) + \phi_{E^{\perp}}(\lambda_1, \lambda_2) \\ &\quad = -tr_1^m(\gamma^{-\frac{1}{r}} \lambda_1^{\frac{1}{r}} \lambda_2) - tr_1^m(\gamma^{-\frac{1}{r}} \delta \lambda_1^{\frac{r+1}{r}}) + \epsilon \\ &\qquad + (p - b)[\delta \lambda_1 + \lambda_2]^{p^m - 1} + b. \end{aligned}$$

Proof It was already shown that the restriction of $f(x_1, x_2)$ to E is ϵ, which corresponds to the case of $\underline{a} = \underline{0}$ in Theorem 9. Thus the function $f(x_1, x_2) + \phi_E(x_1, x_2)$ becomes a generalized regular bent function from (36) and (38) and its trace transform can be derived from (37), (39), and Theorem

9. It was also shown that the restriction of $\tilde{f}(\lambda_1, \lambda_2)$ to $E^{\perp}$ defined in (35) is also affine, that is, ϵ and from (37), (39), and Theorem 9, $\tilde{f}(\lambda_1, \lambda_2)$ also becomes a generalized regular bent function. □

References

[1] L.D. Baumert, Cyclic Difference Sets, Lecture Notes in Mathematics, vol.182, Springer Verlag, New York, 1971.

[2] C. Carlet, "Two new classes of bent functions," Proc. EUROCRYPT'93, Lecture Notes in Computer Science, vol.765, pp.77–101, Springer-Verlag, Berlin, Germany, 1994.

[3] C. Carlet, "Generalized partial spreads," IEEE Trans. Inf. Theory, vol.41, no.5, pp.1482–1487, Sept. 1995.

[4] J.F. Dillon, Elementary Hadamard difference sets, Ph.D. Dissertation, University of Maryland, 1974.

[5] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," Proc. 1994 Leuven Workshop on Cryptographic Algorithms, Lecture Notes in Computer Science, vol.1008, pp.61–74, Springer-Verlag, Berlin, Germany, 1995,

[6] S. Kim, G.-M. Gil, K.H. Kim, and J.-S. No, "Generalzed bent functions constructed from partial spreads," preprint, 2001.

[7] P.V. Kumar, R.A. Scholtz, and L.R. Welch, "Generalized bent functions and their properties," J. Comb. Theory A., vol.40, pp.90–107, 1985.

[8] A. Lempel and M. Cohn, "Maximal families of bent sequences," IEEE Trans. Inf. Theory, vol.28, no.6, pp.865–868, Nov. 1982.

[9] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications, vol.20, Addison-Wesley, Reading, MA, 1983.

[10] F.J. McWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, New York, 1977.

[11] J.D. Olsen, R.A. Scholtz, and L.R. Welch, "Bent-function sequences," IEEE Trans. Inf. Theory, vol.28, no.6, pp.858–864, Nov. 1982.

[12] O.S. Rothaus, "On bent functions," J. Comb. Theory A., vol.20, pp.300–305, 1976.

[13] G. Seroussi and A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields," SIAM J. Comput., vol.9, no.4, pp.758–767, Nov. 1980.

[14] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, Spread Spectrum Communications, vol.1, Computer Science Press, Rockville, MD, 1985.

[15] J. Wolfmann, "Bent functions and coding theory," Proc. Difference Sets, Sequences and their Correlation Properties, NATO Advanced Study Institute Workshop, pp.393–418, Bad Windshiem, Germany, Aug. 1998.

Sunghwan Kim received the B.S. and M.S.E.E. degrees in the School of Electrical Engineering, Seoul National University, in 1999 and 2001, respectively. Currently, he is a Ph.D. candidate in the School of Electrical Engineering and Computer Science, Seoul National University. His research interests include error-correcting codes, pseudo random sequences, low-density parity-check (LDPC) codes, wireless communications, and communications theory.

Gang-Mi Gil received the B.S. and M.S.E.E. degrees in the School of Electrical Engineering, Seoul National University, in 2000 and 2002, respectively. Currently, she is a research engineer of Samsung electronics. Her research interests include error-correcting codes, pseudo random sequences, low-density parity-check (LDPC) codes, wireless communications, and communications theory.

Jong-Seon No received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1988. He was a Senior MTS at Hughes Network Systems from February 1988 to July 1990. He was also an Associate Professor in the Department of Electronic Engineering, Konkuk University, Seoul, Korea, from September 1990 to July 1999. He joined the faculty of the School of Electrical Engineering and Computer Science, Seoul National University, in August 1999, where he is currently an Associate Professor. His area of research interests includes error-correcting codes, sequences, cryptography, space-times codes, LDPC codes, and wireless communication systems.