Partial Spread를 이용한 일반화된 Bent함수

김성환, 길강미, 김경희, 노종선*
*서울대학교, 전기컴퓨터공학부

Generalized Bent Functions Constructed From Partial Spreads

Sunghwan Kim, Gang-Mi Gil,
Kyung-Hee Kim and Jong-Seon No*
*School of Electrical Engineering
and Computer Science
Seoul National Univ.

ABSTRACT

In this paper, for $n = 2m$ and odd prime p, new generalized bent functions from the finite field F_{p^n} to the prime field F_p are constructed from the partial spreads for F_{p^n}. Closed form expressions for the proposed generalized bent functions and their trace transform are derived in the form of the trace functions. The trace expressions for the bent functions and their trace transforms defined on F_{2^m} constructed by using PS$-$ are also derived.

I. INTRODUCTION

Rothaus introduced *bent functions* defined on the n-tuple binary vector space into F_2 [4]. Boolean functions on the n-tuple binary vector space are called bent functions if their Fourier coefficients only take the values $+1$ or -1. One of the well-known classes of bent functions is the class of Maiorana-McFarland, called class M. Dillon constructed elementary Hadamard difference sets by using partial spreads for a group of square order, called PS$-$ and PS$+$, whose characteristic functions correspond to the bent functions [2]. Several other classes of bent functions are introduced by Carlet, called class D, class C and generalized partial spreads (GPS) [1]. Kumar, Scholtz and Welch introduced generalized bent functions from the q-ary vector space to the set of integers modulo q, whose Fourier coefficients all have unit magnitude [3]. They constructed several generalized bent functions in their paper. In this paper, for $n = 2m$ and odd prime p, new generalized bent functions from the finite field F_{p^n} to the prime field F_p are constructed from the partial spreads for F_{p^n}. Closed form expressions for the proposed generalized bent functions and their trace transform are derived in the form of the trace functions. The trace expressions for the bent functions and their trace transforms defined on F_{2^m} constructed by using PS$-$ are also derived.

II. PRELIMINARIES

Let q be an 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 the function $f(\underline{x})$ is defined as

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

where $\underline{x}^T$ denotes the transpose of $\underline{x}$. Then the generalized bent function is defined as [3]:

Definition 1 : 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 the Fourier coefficients of the generalized bent function are integral powers of ω, i.e.,

$$F(\underline{\lambda}) = \omega^{\tilde{f}(\underline{\lambda})}, \quad \text{all } \underline{\lambda} \in V_q^n, \tag{2}$$

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 paper, it is only considered that the integer q is odd prime p. Thus, V_p^n is the n-dimensional vector space over the finite field F_p with p elements and $f(\underline{x})$ is a function from V_p^n to F_p.

Let F_{p^n} be a finite field with p^n elements. Let $n = em > 1$ for some positive integers e and m. Then a trace function $\mathrm{tr}_m^n(\cdot)$ is a mapping from F_{p^n} to its subfield F_{p^m} defined as $\mathrm{tr}_m^n(x) = \sum_{i=0}^{e-1} x^{p^{mi}}$, where x is an element in F_{p^n}.

Olsen, Scholtz and Welch introduced the *trace transform* for functions from F_{2^n} to F_2. Then the trace transform for a function from F_{p^n} to F_p can be generalized as follows:

Definition 2 : Let $f(x)$ be a function from F_{p^n} to F_p. Then the *trace transform* of $f(x)$ and its inverse transform are defined by

$$\begin{aligned} F(\lambda) &= \frac{1}{\sqrt{p^n}} \sum_{x\in F_{p^n}} \omega^{f(x)-\mathrm{tr}_1^n(\lambda\cdot x)}, \quad (3) \\ &\quad \text{all } \lambda \in F_{p^n} \\ \omega^{f(x)} &= \frac{1}{\sqrt{p^n}} \sum_{\lambda\in F_{p^n}} F(\lambda)\cdot\omega^{\mathrm{tr}_1^n(\lambda\cdot x)}, \\ &\quad \text{all } x \in F_{p^n}. \end{aligned}$$

□

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

$$\begin{aligned} x &= \sum_{i=1}^n x_i\cdot\alpha_i \Rightarrow \underline{x} = (x_1, x_2, \cdots, x_n) \\ \lambda &= \sum_{i=1}^n \lambda_i\cdot\alpha_i \Rightarrow \underline{\lambda} = (\lambda_1, \lambda_2, \cdots, \lambda_n), \end{aligned}$$

where x_i and λ_i are in F_p and $\{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n\}$ is some basis of F_{p^n} over F_p. By replacing x in F_{p^n} by $\underline{x}$ in V_p^n, the function $f(x)$ from F_{p^n} to F_p makes the corresponding function $f(\underline{x})$ from V_p^n to F_p.

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

$$\mathrm{tr}_1^n(\alpha_i\cdot\alpha_j) = \begin{cases} a_i, & \text{if } i = j \\ 0, & \text{otherwise,} \end{cases} \tag{4}$$

where $a_i \in F_p^*$. It is known that for any positive integer n and odd prime p, there exists trace-orthogonal basis of F_{p^n} over F_p [5].

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

$$\mathrm{tr}_1^n(\lambda \cdot x) = \sum_{i=1}^{n} a_i \cdot \lambda_i \cdot x_i. \quad (5)$$

Let $\lambda_j^{'} = a_i \cdot \lambda_i$ for $i, 1 \le i \le n$ and $\underline{\lambda}^{'} = (\lambda_1^{'}, \lambda_2^{'}, \lambda_3^{'}, \cdots, \lambda_n^{'})$. Then the relation in (5) can be rewritten as

$$\mathrm{tr}_1^n(\lambda \cdot x) = \sum_{i=1}^{n} \lambda_i^{'} \cdot x_i = \underline{\lambda}^{'} \cdot \underline{x}^T. \quad (6)$$

It is clear that the Fourier transform of a function $f(\underline{x})$ from V_p^n to F_p is related to the trace transform of the corresponding function $f(x)$ from F_{p^n} to F_p as follows: $F(\lambda) = F(\underline{\lambda}^{'})$. That is, the set of the trace transform values of the function $f(x)$ is the same as that of the Fourier coefficients of the corresponding function $f(\underline{x})$. Therefore, if the trace transform values of the function $f(x)$ only take the values of unit magnitude, the corresponding function $f(\underline{x})$ becomes the generalized bent function. Now, a function $f(x)$ defined on F_{p^n} is called generalized bent function if the trace transform of $f(x)$ only takes the values of unit magnitude.

Let G be a group of square order M^2. Let H_i's be subgroups of order M of a group G. Dillon defined a family of subgroups $H_1, H_2, \cdots, H_N$ as a *partial spread* for G if they are pairwise disjoint (except for 0), that is, for $i \neq j$, $H_i \cap H_j = \{0\}$. If $N = M+1$, it is called a *spread*. Using the partial spread for the group G, Dillon constructed elementary Hadamard difference sets, so called PS− and PS+. He also showed that if a partial spread is defined for the even dimensional binary vector space V_2^{2m}, the characteristic functions of PS− and PS+ become bent functions defined on the even dimensional binary vector space V_2^{2m}. In the next section, for odd prime p, generalized bent functions from F_{p^n} to F_p are constructed using the partial spread defined for the finite field F_{p^n}.

III. Construction of Generalized Bent Functions

Let $n = 2m$ and F_{p^n} be the finite field with p^n elements. Let $T = p^m + 1$ and α be a primitive element of F_{p^n}. Then α^T is a primitive element of F_{p^m}. Let H_i's be additive subgroups of order p^m of F_{p^n} defined by

$$\begin{aligned} H_0 &= \{\eta\alpha^0 | \eta \in F_{p^m}\} \\ H_i &= \{\eta\alpha^i | \eta \in F_{p^m}\},\ 1 \le i \le T-1 \quad (7) \end{aligned}$$

and we also define $H_i^* = H_i \backslash \{0\}$, $0 \le i \le T-1$. It is clear that for all $i \neq j$, $0 \le i, j \le T-1$, $H_i \cap H_j = \{0\}$ and $F_{p^n} = \bigcup_{i=0}^{T-1} H_i$. Then the family of subgroups given by

$$H_0, H_1, H_2, \cdots, H_{T-1}$$

makes a spread for F_{p^n}. Let T_s be the set of integers modulo T, i.e. $\{0, 1, 2, \cdots, T-1\}$ and I_k's be any disjoint subsets given by

$$I_k \subset T_s,\ \ 0 \le k \le p-1, \quad (8)$$

where the cardinality of the subsets I_k is given as $|I_0| = p^{m-1} + 1$ and $|I_k| = p^{m-1}$ for k, $1 \le k \le p-1$. That is, for all $k \neq l, 0 \le k, l \le p-1$, $I_k \cap I_l = \phi$ and $\bigcup_{k=0}^{p-1} I_k = T_s$. And we also define the subsets $\bar{I}_k$'s of the integer set T_s as

$$\bar{I}_k = \{\frac{T}{2} - i \mod T \mid i \in I_k\},\ \ 0 \le k \le p-1. \quad (9)$$

It is clear that for all $k \neq l$, $0 \le k, l \le p-1$, $\bar{I}_k \cap \bar{I}_l = \phi$ and $\bigcup_{k=0}^{p-1} \bar{I}_k = T_s$.

Using the partial spreads for F_{p^n}, we can make a family of subsets D_k's of F_{p^n} given as

$$D_0 = \bigcup_{i \in I_0} H_i$$
$$D_k = \bigcup_{i_k \in I_k} H^*_{i_k}, \quad 1 \le k \le p-1, \quad (10)$$

where the subsets I_k's are defined in (8). It is clear that for all $k \neq l, 0 \le k, l \le p-1$, $D_k \cap D_l = \phi$ and $F_{p^n} = \bigcup_{k=0}^{p-1} D_k$. Then we can construct a generalized bent function from the subsets D_k's as in the following theorem:

Theorem 3 : Let D_k's be subsets of F_{p^n} defined in (10), $0 \le k \le p-1$. For odd prime p, the function $f(x)$ from F_{p^n} to F_p defined by

$$f(x) = \begin{cases} 0, & \text{if } x \in D_0 \\ k, & \text{if } x \in D_k, \quad 1 \le k \le p-1 \end{cases} \quad (11)$$

is a regular bent function.

Proof : It is enough to show that the trace transform of $f(x)$ defined in (11) has unit magnitude. The trace transform defined in (4) of $f(x)$ is given as

$$\begin{aligned} F(\lambda) &= \frac{1}{\sqrt{p^n}} \sum_{x \in F_{p^n}} \omega^{f(x) - \mathrm{tr}_1^n(\lambda \cdot x)} \\ &= \frac{1}{\sqrt{p^n}} [\sum_{x \in D_0} \omega^{-\mathrm{tr}_1^n(\lambda \cdot x)} \\ &\quad + \omega \sum_{x \in D_1} \omega^{-\mathrm{tr}_1^n(\lambda \cdot x)} \\ &\quad + \cdots \\ &\quad + \omega^{p-1} \sum_{x \in D_{p-1}} \omega^{-\mathrm{tr}_1^n(\lambda \cdot x)}]. \end{aligned}$$

For $\lambda = 0$, it is clear that $F(\lambda) = 1$. Now, we have to prove for $\lambda \neq 0$. Let α be a primitive element in F_{p^n}. Let $x = \delta \cdot \alpha^i, \delta \in F^*_{p^m}$, $i \in T_s$. Then the trace transform can be rewritten as

$$\begin{aligned} F(\lambda) &= \frac{1}{\sqrt{p^n}} [1 + \sum_{i \in I_0} \sum_{\delta \in F^*_{p^m}} \omega^{-\mathrm{tr}_1^m(\delta \cdot \mathrm{tr}_m^n(\alpha^i \cdot \lambda))} \\ &\quad + \omega \sum_{i \in I_1} \sum_{\delta \in F^*_{p^m}} \omega^{-\mathrm{tr}_1^m(\delta \cdot \mathrm{tr}_m^n(\alpha^i \cdot \lambda))} \quad (12) \\ &\quad + \cdots \\ &\quad + \omega^{p-1} \sum_{i \in I_{p-1}} \sum_{\delta \in F^*_{p^m}} \omega^{-\mathrm{tr}_1^m(\delta \cdot \mathrm{tr}_m^n(\alpha^i \cdot \lambda))}]. \end{aligned}$$

The inner summation in the $(k+1)$-th summation in (12) can be given by

$$\sum_{\delta \in F^*_{p^m}} \omega^{-\mathrm{tr}_1^m(\delta \cdot \mathrm{tr}_m^n(\alpha^i \cdot \lambda))} = \begin{cases} p^m - 1, & \text{if } \mathrm{tr}_m^n(\alpha^i \cdot \lambda) = 0 \\ -1, & \text{otherwise.} \end{cases} \quad (13)$$

Thus we have to find the case when $\mathrm{tr}_m^n(\alpha^i \cdot \lambda) = 0$.

For odd prime p, we have the relation

$$\begin{aligned} \mathrm{tr}_m^n(\alpha^{\frac{T}{2}}) &= \alpha^{\frac{p^m+1}{2}} + \alpha^{p^m \cdot \frac{p^m+1}{2}} \\ &= \alpha^{\frac{p^m+1}{2}} + \alpha^{\frac{p^{2m}+p^m}{2}} \\ &= \alpha^{\frac{p^m+1}{2}} + \alpha^{\frac{p^{2m}-1}{2}} \cdot \alpha^{\frac{p^m+1}{2}} \\ &= 0 \end{aligned}$$

and for any integer i, $\mathrm{tr}_m^n(\alpha^{\frac{T}{2}+iT}) = \alpha^{iT} \cdot \mathrm{tr}_m^n(\alpha^{\frac{T}{2}})$. From the balance property of $\mathrm{tr}_m^n(\alpha^t)$, $\mathrm{tr}_m^n(\alpha^t) = 0$ occurs $p^m - 1$ as t varies over $0 \le t \le p^n - 2$. Therefore, as t varies over $0 \le t \le T-1$, $\mathrm{tr}_m^n(\alpha^t) = 0$ occurs once when $t = \frac{T}{2}$.

Let $\lambda = \epsilon \cdot \alpha^j, \epsilon \in F^*_{p^m}, j \in T_s$. Then

$$\begin{aligned} \mathrm{tr}_m^n(\alpha^i \cdot \lambda) &= \delta\epsilon \cdot \mathrm{tr}_m^n(\alpha^{i+j}) \\ &= \begin{cases} 0, & j \in \bar{I}_k \\ \neq 0, & \text{otherwise.} \end{cases} \quad (14) \end{aligned}$$

Using (13) and (14), the $(k+1)$-th double summation in (12) can be written as

$$\sum_{i \in I_k} \sum_{\delta \in F^*_{p^m}} \omega^{-\mathrm{tr}_1^m(\delta \cdot \mathrm{tr}_m^n(\alpha^i \cdot \lambda))}$$

$$= \begin{cases} -|I_k| & \text{if } j \notin \bar{I}_k \\ p^m - |I_k| & \text{if } j \in \bar{I}_k . \end{cases} \quad (15)$$

For a given nonzero λ, j belongs to the only one subset $\bar{I}_k$. If $j \in \bar{I}_0$, then the trace transform of $f(x)$ is calculated as

$$\begin{aligned} F(\lambda) &= \frac{1}{\sqrt{p^n}}(1 + p^m - p^{m-1} - 1 \\ &\quad -p^{m-1}\omega - p^{m-1}\omega^2 \\ &\quad - \cdots - p^{m-1}\omega^{p-1}) \\ &= 1. \end{aligned} \quad (16)$$

If $j \in \bar{I}_k, 1 \leq k \leq p-1$, then the trace transform of $f(x)$ is

$$\begin{aligned} F(\lambda) &= \frac{1}{\sqrt{p^n}}(1 - p^{m-1} - 1 - p^{m-1}\omega \\ &\quad -p^{m-1}\omega^2 - \cdots - p^{m-1}\omega^{k-1} \\ &\quad +p^m\omega^k - p^{m-1}\omega^k - p^{m-1}\omega^{k+1} \\ &\quad - \cdots - p^{m-1}\omega^{p-1}) \\ &= \omega^k. \end{aligned} \quad (17)$$

Thus, for all $\lambda \in F_{p^n}$, $F(\lambda)$ is integral power of ω and $f(x)$ is the regular bent function. □

From the subset D_i's defined in (10), $0 \leq i \leq p-1$, we can define $\bar{D}_i$ as a subset of F_{p^n} as $\bar{D}_0 = \bigcup_{i \in \bar{I}_0} H_i$ and $\bar{D}_k = \bigcup_{i \in \bar{I}_k} H_i^*$, $1 \leq k \leq p-1$.

From the equations (16) and (17), the Fourier transform $\tilde{f}(\lambda)$ of the generalized bent functions defined in (11) can be derived as in the following theorem.

Theorem 4 : For odd prime p, the Fourier transform $\tilde{f}(\lambda)$ of the generalized bent functions defined in (11) is given by

$$\tilde{f}(\lambda) = \begin{cases} 0, & \text{if } \lambda \in \bar{D}_0 \\ k, & \text{if } \lambda \in \bar{D}_k, \quad 1 \leq k \leq p-1. \end{cases} \quad (18)$$

□

It is easy to derive that the trace function from F_{p^n} to F_{p^m} has the relation as

$$[\mathrm{tr}_m^n(x)]^{p^m-1} = \begin{cases} 0, & x \in H_{\frac{T}{2}} \\ 1, & \text{otherwise.} \end{cases}$$

Using the above equation, we can define the characteristic function $\Phi_{H_i}(x)$ for the subgroup H_i in (7) as

$$\Phi_{H_i}(x) = \begin{cases} 1, & x \in H_i \\ 0, & \text{otherwise.} \end{cases}$$

Then the function $\Phi_{H_i}(x)$ is given by

$$\Phi_{H_i}(x) = 1 - \left[\mathrm{tr}_m^n(x \cdot \alpha^{-i+\frac{T}{2}})\right]^{p^m-1}, \quad (19)$$

where $0 \leq i \leq T-1$. Using the characteristic function (19), the generalized bent function defined in (11) and its Fourier transform can be rewritten as in the following corollary.

Corollary 5 : The generalized bent function $f(x)$ defined (11) and its Fourier transform $\tilde{f}(\lambda)$ are given by

$$\begin{aligned} f(x) &= \sum_{k=0}^{p-1} \sum_{i_k \in I_k} \{k \\ &\quad +(-k) \cdot \left[\mathrm{tr}_m^n(x \cdot \alpha^{-i_k+\frac{T}{2}})\right]^{p^m-1}\} \end{aligned} \quad (20)$$

$$\begin{aligned} \tilde{f}(\lambda) &= \sum_{k=0}^{p-1} \sum_{i_k \in \bar{I}_k} \{k \\ &\quad +(-k) \cdot \left[\mathrm{tr}_m^n(\lambda \cdot \alpha^{-i_k+\frac{T}{2}})\right]^{p^m-1}\}. \end{aligned} \quad (21)$$

□

Using the trace-orthogonal basis defined in (4), the generalized bent function $f(x)$ defined on F_{p^n} in Corollary 5 and (21) can be transformed into the generalized bent function $f(\underline{x})$ defined on the vector space V_p^n.

For $p = 2$, Theorem 3 and Corollary 5 can be applied to construct bent functions if we replace the equation (19) by $\Phi_{H_i}(x) = 1 - \left[\mathrm{tr}_m^n(x \cdot \alpha^{-i})\right]^{2^m-1}, 0 \le i \le T-1$, where $T = 2^m+1$, because $\mathrm{tr}_m^n(\alpha^T) = 0$. Let I_1 be any subset with $|I_1| = 2^{m-1}$ of the set $T_s = \{0, 1, 2, \cdots, 2^m\}$ and $\bar{I}_1 = \{T-i \mod T | i \in I_1\}$. Then a bent function defined on F_{2^n} constructed by using PS− and its Fourier transform can be expressed as

$$f(x) = \sum_{i \in I_1} \left[\mathrm{tr}_m^n(x \cdot \alpha^{-i})\right]^{2^m-1} \qquad (22)$$

$$\tilde{f}(\lambda) = \sum_{i \in \bar{I}_1} \left[\mathrm{tr}_m^n(\lambda \cdot \alpha^{-i})\right]^{2^m-1}. \qquad (23)$$

The bent function defined in (22) can be simplified as in the following theorem.

Theorem 6 : Let $n = 2m$. The bent function $f(x)$ defined in (22) can be expressed as

$$f(x) = \sum_{k=1}^{2^{m-1}} \mathrm{tr}_m^n\{x^{(2k-1)(2^m-1)} \cdot \sum_{i \in I_1} \alpha^{-i\cdot(2k-1)(2^m-1)}\}. \qquad (24)$$

Proof : The inner term of the summation in the bent function $f(x)$ defined on F_{2^n} in (22) can be expanded as

$$\left[\mathrm{tr}_m^n(x \cdot \alpha^{-i})\right]^{2^m-1} = \sum_{j_1=0}^{1}\sum_{j_2=0}^{1}\cdots\sum_{j_{m-1}=0}^{1} \mathrm{tr}_m^n\left((\alpha^{-i}x)^{1+2^{m\cdot j_1+1}+\cdots+2^{m\cdot j_{m-1}+m-1}}\right).$$

Thus, the bent function $f(x)$ can be expressed as

$$f(x) = \sum_{j_1=0}^{1}\sum_{j_2=0}^{1}\cdots\sum_{j_{m-1}=0}^{1} \mathrm{tr}_m^n\{x^{1+2^{m\cdot j_1+1}+\cdots+2^{m\cdot j_{m-1}+m-1}} \cdot \sum_{i \in I_1} \alpha^{-i\cdot(1+2^{m\cdot j_1+1}+\cdots+2^{m\cdot j_{m-1}+m-1})}\}.$$

The exponent of x is simplified as $A = (2^m - 1) \cdot a$, where $(1, j_1, j_2, j_3, \cdots, j_{m-1})$ is a 2-adic expansion of a, $1 \le a \le 2^m - 1$ given by

$$a = 1 + j_1 \cdot 2 + j_2 \cdot 2^2 + \cdots + j_{m-1} \cdot 2^{m-1}.$$

□

REFERENCES

[1] C. Carlet, "Two new classes of bent functions," in *Proc. EURO-CRYPT'93 (Lecture Notes in Computer Science 765)*, pp.77-101, 1994.

[2] J.F. Dillon, "Elementary Hadamard difference sets," Ph.D. dissertation, University of Maryland, 1974.

[3] P.V. Kumar, R.A. Scholtz and L.R. Welch, "Generalized bent functions and their propertes," *Journal of Combinatorial Theory*, Series A. vol. 40, pp.90-107, 1985.

[4] O.S. Rothaus, "On bent functions," *Journal of Combinatorial Theory*, Series A. vol. 20, pp.300-305, 1976.

[5] G. Seroussi and A. Lempel, "Factorization of Symmetric Matrices and trace-orthogonal bases iin finite fields," *SIAM J. Comput.*, vol. 9, no. 4, pp. 758-767, Nov. 1980.

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