# Generalized Bent Functions Constructed From Partial Spreads

Sunghwan Kim, Gang-Mi Gil, Kyung-Hee Kim and Jong-Seon No
School of EECS, Seoul National University, Seoul, Korea
e-mail: nodoubt@snu.ac.kr, cominkil@ccl.snu.ac.kr, khkim@math.snu.ac.kr, jsno@snu.ac.kr

*Abstract* — **In this paper, new generalized bent functions from the finite field $F_{p^n}$ to the prime field $F_p$ are constructed from partial spreads for $n = 2m$ and odd prime $p$.**

## I. Introduction

Rothaus introduced *bent functions* defined on the $n$-tuple binary vector space into $F_2$ [3]. 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 [1]. Let $V_q^n$ be an $n$-dimensional vector space over a set of integers modulo $q$, $J_q$ and let $\omega = e^{j\frac{2\pi}{q}}$, $j = \sqrt{-1}$. Let $f(\underline{x})$ be a function from $V_q^n$ to $J_q$. Using the Fourier transform of the function $f(\underline{x})$ defined by

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

the generalized bent functions are defined as:

**Definition 1** [Kumar, Scholtz and Welch [2]] : 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 $\underline{\lambda} \in V_q^n$.

## II. Generalized Bent Functions

Let $n = 2m$ and $F_{p^n}$ be a finite field with $p^n$ elements. Let $T = p^m + 1$ and $\alpha$ be a primitive element of $F_{p^n}$. Then $\alpha^T$ 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

$$H_i = \{\eta\alpha^i \mid \eta \in F_{p^m}\}, \quad 0 \le i \le T-1 \tag{1}$$

and we also define $H_i^* = H_i\backslash\{0\}$, $0 \le i \le T-1$. It is clear that for all $i \ne j$, $0 \le i,j \le T-1$, $H_i \cap H_j = \{0\}$ 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 a set of integers modulo $T$, i.e. $\{0,1,2,\cdots,T-1\}$ and $I_k$'s be any disjoint subsets given by $I_k \subset T_s$, $0 \le k \le p-1$, 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 $k \ne l, 0 \le k,l \le p-1$, $I_k \cap I_l = \phi$ 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

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

It is clear that for all $k \ne l$, $0 \le k,l \le p-1$, $\bar{I}_k \cap \bar{I}_l = \phi$ 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 $D_i$'s of $F_{p^n}$ given as

$$D_0 = \bigcup_{i\in I_0} H_i, \quad D_k = \bigcup_{i_k\in I_k} H_{i_k}^*, \quad 1 \le k \le p-1. \tag{3}$$

It is clear that for all $k \ne l, 0 \le k,l \le p-1$, $D_k \cap D_l = \phi$ and $F_{p^n} = \bigcup_{k=0}^{p-1} D_k$. Then we can construct a generalized bent function from the sets $D_i$'s as in the following theorem:

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

**Theorem 2** : Let $D_k$'s be subsets of $F_{p^n}$ defined in (3), $0 \le k \le p-1$. For odd prime $p$, the function $f(x)$ from $F_{p^n}$ to $F_p$ defined by

$$f(x) = \begin{cases} 0, & \text{if } x \in D_0 \\ k, & \text{if } x \in D_k, \quad 1 \le k \le p-1 \end{cases} \tag{4}$$

is a regular bent function.

From the subset $D_i$'s defined in (3), $0 \le i \le p-1$, 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 $\bar{D}_k = \bigcup_{i\in\bar{I}_k} H_i^*$, $1 \le k \le p-1$. Thus, the Fourier transform $\tilde{f}(\lambda)$ of the generalized bent functions defined in (4) can be derived as in the following theorem.

**Theorem 3** : For odd prime $p$, the Fourier transform $\tilde{f}(\lambda)$ of the generalized bent functions defined in (4) is given by

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

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 (1) 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

$$\Phi_{H_i}(x) = 1 - \left[\mathrm{tr}_m^n(x \cdot \alpha^{-i+\frac{T}{2}})\right]^{p^m-1}, \quad 0 \le i \le T-1. \tag{5}$$

Using the characteristic function (5), the generalized bent function defined in (4) and its Fourier transform can be rewritten as in the following corollary.

**Corollary 4** : The generalized bent function $f(x)$ defined (4) and its Fourier transform $\tilde{f}(\lambda)$ are given by

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

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

For $p = 2$, the binary bent function defined from the partial spread can be simplified as in the following theorem.

**Theorem 5** : Let $n = 2m$. The binary bent function $f(x)$ defined from partial spread can be expressed as

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

## References

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

[2] 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.

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



0-7803-7501-7/02/$17.00©2002 IEEE.