New classes of generalized bent functions

Bimal Mandal

Department of Mathematics
Indian Institute of Technology Roorkee
Roorkee, India

This is a joint work with Pantelimon Stănică and Sugata Gangopadhyay

Boolean Functions and Their Application (BFA)
Norway, July 3-8, 2017

July 7, 2017
Outlines

- Introduction
- Subspace sum of a generalized Boolean function and their properties
- Construction of $D^p$, $D_0^p$ and $C^p$ classes of bent functions
- Existence and nonexistence of $C^p$ class of bent functions
- References
Generalized Boolean functions

- $\mathbb{F}_p = \{0, 1, \ldots, p - 1\}$ is a field of characteristic $p$.
- $\mathbb{F}_{p^n}$ is an extension field of degree $n$ over $\mathbb{F}_p$.
- $\mathbb{F}_{p}^n = \{x = (x_1, \ldots, x_n) : x_i \in \mathbb{F}_p\}$ is a vector space over $\mathbb{F}_p$.
- It can be checked that $x = (x_1, x_2, \ldots, x_n) \mapsto x_1 a_1 + x_2 a_2 + \cdots + x_n a_n$ is an $\mathbb{F}_p$-vector space isomorphism from $\mathbb{F}_{p}^n$.
- Any function $f : \mathbb{F}_{p}^n \longrightarrow \mathbb{F}_p$ is said to be a generalized Boolean function.
- $\mathcal{B}_n^p$ = the set of all generalized Boolean functions on $n$ variables.
- $\text{Tr}_1^n : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$ is defined by

$$\text{Tr}_1^n(x) = x + x^p + x^{p^2} + \ldots + x^{p^{n-1}}.$$
Any $f \in \mathcal{B}_n^p$ can be uniquely expressed as

$$f(x_1, x_2, \ldots, x_n) = \sum_{a=(a_1, \ldots, a_n) \in \mathbb{F}_p^n} \mu_a \left( \prod_{i=1}^n x_i^{a_i} \right).$$

The algebraic degree of $f \in \mathcal{B}_n^p$ is defined as

$$\deg(f) = \max_{a \in \mathbb{F}_p^n} \left\{ \sum_{i=1}^n a_i : \mu_a \neq 0 \right\}.$$
The generalized Walsh–Hadamard transform of \( f \in B_n^p \) at \( a \in \mathbb{F}_p^n \) is defined as

\[
\mathcal{H}_f(a) = \sum_{x \in \mathbb{F}_p^n} \zeta^{f(x) - a \cdot x}.
\]

\( f \in B_n^p \) is called generalized bent function if

\[
|\mathcal{H}_f(a)| = p^n^2 \text{ for all } a \in \mathbb{F}_p^n.
\]

\( f \in B_n^p \) is a generalized bent function if for all \( 0 \neq a \in \mathbb{F}_p^n \)

\[
\sum_{x \in \mathbb{F}_p^n} \zeta^{f(x+a)-f(x)} = 0.
\]

The derivative of \( f \in B_n^p \) with respect to \( a \in \mathbb{F}_p^n \) is defined as

\[
D_a f(x) = f(x + a) - f(x) \text{ for all } x \in \mathbb{F}_p^n.
\]
A class of bent functions is complete if it is globally invariant under the action of the general affine group and under the addition of affine functions.

\[ \Omega_f = (f(x_0), f(x_1), \ldots, f(x_{p^n-1})), f \in B_n^p. \]

\( \mathcal{R}_p(r, n) = \) the set of all codewords \( \Omega_f \), where \( f \in B_n^p \) with \( \deg(f) \leq r \) and \( 0 \leq r \leq n(p - 1) \).

Let \( \mathcal{A} \) be a group algebra of \( \mathbb{F}_p^n \) over the field \( \mathbb{F}_p \). An element \( x \in \mathcal{A} \) can be expressed as

\[ x = \sum_{g \in \mathbb{F}_p^n} x_g X^g, \text{ where } x_g \in \mathbb{F}_p. \]
ψ : A → F_p is defined by

\[ x = \sum_{g \in F_p^n} x_g X^g \mapsto \sum_{g \in F_p^n} x_g \text{ for all } x \in A. \]

\[ \mathcal{P} = \{ x \in A : \psi(x) = 0 \} = \{ x \in A : \sum_{g \in F_p^n} x_g = 0 \} \text{ is the maximal ideal of } A. \]

\[ A = \mathcal{P}^0 \supset \mathcal{P} \supset \mathcal{P}^2 \supset \ldots \supset \mathcal{P}^{n(p-1)} = F_p. \]

\[ \mathcal{P}^i \mathcal{P}^j = \mathcal{P}^{i+j} \text{ and } \mathcal{P}^{n(p-1)+1} = \{ 0 \}. \]

\[ f \in B_n^p \text{ can be identified with the codeword } \Omega_f = \sum_{g \in F_p^n} f(g) X^g. \]
For any elements $a, b \in \mathbb{F}_p^n$, we have [Carlet, Eurocrypt’93]

$$
\sum_{x \in -a+E} \zeta^f(x) - b \cdot x = p^{\dim E} - \frac{n}{2} \zeta^{a \cdot b} \sum_{x \in b+E_\perp} \zeta^{\tilde{f}(x) - a \cdot x},
$$

where $\zeta = e^{\frac{2\pi i}{p}}$ is the $p^{th}$ complex root of unity.

The function $f : \mathbb{Z}_q^n \times \mathbb{Z}_q^n \rightarrow \mathbb{Z}_q$ of the form [Carlet, Eurocrypt’93]

$$
f(x, y) = x \cdot \pi(y) + \frac{q}{2} \phi_E(x, y)
$$

is bent, where $x \cdot \pi(y) = 0$ for all $(x, y) \in E$. 


Subspace sum of a function

- \( V = \langle a_1, \ldots, a_k \rangle = \{ a \in \mathbb{F}_p^n : a = \sum_{i=1}^{k} c_i a_i, c_i \in \mathbb{F}_p, 1 \leq i \leq k \} \).

- **Subspace sum of** \( f \in B_p^n \) **with respect to** \( V \) **is defined as**

\[
S_V f(x) = \sum_{u \in V} f(x + u) \text{ for all } x \in \mathbb{F}_p^n.
\]

**Example**

Let \( f \in B_3^n \) and \( V = \langle a \rangle \). Then \( S_V f(x) = f(x + 2a) + f(x + a) + f(x) \).

**Remark**

Let \( i \in \{0, 1, \ldots, p - 1\} \) and \( V = \langle a \rangle, 0 \neq a \in \mathbb{F}_p^n \). Then

\[
S_V f(x) = S_V f(x + ia). \tag{1}
\]
The $k$-th derivative

**Lemma**

Let $k \leq p$ be a positive integer and $f \in \mathcal{B}_n^p$. Then for any $a \in \mathbb{F}_p^n$,

$$D_a D_a \ldots D_a f(x) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} f(x + (k - i)a) \text{ for all } x \in \mathbb{F}_p^n.$$  \hspace{1cm} (2)
The $k$-th derivative and the subspace sum I

**Theorem**

Let $V = \langle a \rangle$ and $f \in B_n^p$. Then $S_V f(x) = \underbrace{D_a D_a \cdots D_a}_{(p-1)-times} f(x)$ for all $x \in \mathbb{F}_p^n$.

Furthermore, for any $r \in \{0, 1, 2, \ldots, p-1\}$

$$r S_V f(x) = D_{ra} \underbrace{D_a \cdots D_a}_{(p-2)-times} f(x)$$

for all $x \in \mathbb{F}_p^n$.

**Example**

Let $f \in B_n^p$ and $V = \langle a \rangle$. Then

$$S_V f(x) = f(x + 2a) + f(x + a) + f(x) = D_a D_a f(x)$$

$$2 S_V f(x) = 2D_a D_a f(x) = D_{2a} D_a f(x) = D_a D_{2a} f(x).$$
More on $k$-th derivative and the subspace sum

Theorem

Let $V$ be a $k$-dimensional subspace of $\mathbb{F}_p^n$ generated by $a_1, a_2, \ldots, a_k$ and $f \in B_n^p$. Then

$$S_Vf(x) = \underbrace{D_{a_1} \cdots D_{a_1}}_{(p-1)-times} \cdots \underbrace{D_{a_k} \cdots D_{a_k}}_{(p-1)-times} f(x).$$
Codes and the subspace sum

Proposition

Let $V$ be a $k$-dimensional subspace of $\mathbb{F}_p^n$ generated by $a_1, a_2, \ldots, a_k$. Let $f \in \mathbb{B}^p_n$ be any function of degree $r$ and $h(x) = S_V f(x), x \in \mathbb{F}_p^n$. Then $(\sum_{v \in V} X^v) \Omega_f$ is the associated codeword of $S_V f$, that is,

$$
\Omega_h = \left( \sum_{v \in V} X^v \right) \Omega_f.
$$

Proposition

Let $V$ be a $k$-dimensional subspace of $\mathbb{F}_p^n$ and $f \in \mathbb{B}^p_n$ of degree $r$. Then the degree of $S_V f$ is less than or equal to $r - k(p - 1)$. In particular, the subspace sum of $f$ with respect to any 1-dimensional subspace of $\mathbb{F}_p^n$ has degree at most $r - p + 1$. 
Theorem

Let $f \in \mathcal{B}_n^p$ and $S_k[f]$ denote the multiset of subspace sum of $f$ with respect to each $k$-dimensional subspace of $\mathbb{F}_p^n$. If $f, h \in \mathcal{B}_n^p$ are affine equivalent, then so are $S_k[f]$ and $S_k[h]$. Precisely, if a nonsingular affine transformation $A$ (operating on $\mathbb{F}_p^n$) map $f$ onto $h$, then it also maps $S_k[f]$ onto $S_k[h]$.

Corollary

If $P$ is any affine invariant for $\mathcal{B}_n^p$, then

$$f \mapsto P\{S_k[f]\}$$

is also an affine invariant for $\mathcal{B}_n^p$. 

Affine equivalence of subspace sums
Theorem

Let $m = 2n$ and $f$ be a generalized Maiorana–McFarland bent function defined as

$$f(x, y) = x \cdot \pi(y) + g(y).$$

Then there exists an $n$-dimensional subspace $E$ of $\mathbb{F}_p^n \times \mathbb{F}_p^n$ such that

1. the subspace sum of $f$ with respect to any one dimensional subspaces of $E$ is 0 if $p$ is odd.
2. the subspace sum of $f$ with respect to any two dimensional subspaces of $E$ is 0 if $p = 2$. 
Some examples

Fact (Helleseth et al., Fact 1)

Any ternary function \( f \) from \( \mathbb{F}_{3^6} \) to \( \mathbb{F}_3 \), defined by

\[
f(x) = \text{Tr}^6_1(\alpha^7 x^{98}),
\]

where \( \alpha \) is a primitive element of \( \mathbb{F}_{3^6} \), is bent and not weakly regular bent.

Theorem

The function \( f \) defined as in Equation (3) does not belong to the complete \( \mathcal{M}^p \) class.

Proof.

Let \( V = \langle a \rangle \), where \( a \in \mathbb{F}_{3^6}^* \). If \( S_V f(x) = 0 \) for all \( x \in \mathbb{F}_{3^6} \), then

\[
2\alpha^7 a^{34} + 3^2 = 0,
\]

which is a contradiction.
## Construction of $\mathcal{D}^p$, $\mathcal{D}_0^p$ and $\mathcal{C}^p$ I

### Theorem

Let $E = E_1 \times E_2$, $E_1, E_2 \subseteq \mathbb{F}_p^n$ with $\dim E_1 + \dim E_2 = n$ and $\epsilon \in \mathbb{F}_p$. The generalized Boolean function $f$ on $\mathbb{F}_p^n \times \mathbb{F}_p^n$ of the form

$$f(x, y) = x \cdot \pi(y) + \epsilon \phi_E(x, y)$$  \hspace{1cm} (4)

is a regular bent, where $\pi$ is a permutation polynomial over $\mathbb{F}_p^n$ such that $\pi(E_2) = E_1^\perp$.

### Remark

The set of all the functions $f$ defined as in Equation (4) is denoted by $\mathcal{D}^p$ and the dual of $f$ is

$$\tilde{f}(x, y) = y \cdot \pi^{-1}(x) + \epsilon \phi_{E^\perp}(x, y).$$
Lemma

Let \( n = 2t \) and \( p \) be an odd prime. Then for all \( x = (x_1, x_2, \cdots, x_n) \), \( y = (y_1, y_2, \cdots, y_n) \in \mathbb{F}_p^n \),

\[
\phi_{E_0}(x, y) = \prod_{i=1}^{n} \prod_{j=1}^{p-1} (x_i - j),
\]

where \( E_0 = \{0\} \times \mathbb{F}_p^n \).
Proof. 

If $x = 0$, then

$$
\prod_{i=1}^{n} \prod_{j=1}^{p-1} (0 - j) = \prod_{i=1}^{n} (p - 1)! = 1 = ((p - 1)!)^n = ((p - 1)!)^{2t}.
$$

We know that $(p - 1)! \equiv -1 \pmod{p}$. (Wilson’s Theorem)

The generalized Boolean function $f$ on $\mathbb{F}_p^n \times \mathbb{F}_p^n$ of the form

$$
f(x, y) = x \cdot \pi(y) + \epsilon \phi_{E_0}(x, y) = x \cdot \pi(y) + \epsilon \prod_{i=1}^{n} \prod_{j=1}^{p-1} (x_i - j) \quad (5)
$$

is a regular bent, where $E_0 = \{0\} \times \mathbb{F}_p^n$. 
Remark
The set of all the functions $f$ defined as in Equation (5) is denoted by $D^p_0$ ($D^p_0 \subset D^p$). If $f \in D^p_0$ is an $m$ variables, then

$$m \equiv 0 \pmod{4}.$$ 

Theorem
In general, $D^p_0$ and $D^p$ are not included in the class $M^p$. Further, the class $M^p$ is in general not included in $D^p_0$ and $D^p$ classes.
Construction of $\mathcal{D}^p$, $\mathcal{D}_0^p$ and $\mathcal{C}^p$ V

Proof.

\[ x \cdot (\pi(y) - \pi_1(y)) = \epsilon(\phi_E(x, y) - \phi_E(0, y)). \quad (\mathcal{D}^p \not\rightarrow \mathcal{M}^p) \]

\[ f(x, y) = x \cdot \psi(y) + g(y) = x \cdot \psi_1(y) + \epsilon\phi_E(x, y) \]

and

\[ g(y) = \epsilon\phi_E(0, y) \in \{0, \epsilon\} \text{ for all } y \in \mathbb{F}_p^n. \quad (\mathcal{M}^p \not\rightarrow \mathcal{D}^p) \]
Construction of $\mathcal{D}^p$, $\mathcal{D}_0^p$ and $\mathcal{C}^p$ VI

**Theorem**

Let $L$ be any linear subspace of $\mathbb{F}_p^n$ and $\pi$ be any permutation on $\mathbb{F}_p^n$ such that for any element $\lambda$ of $\mathbb{F}_p^n$, the set $\pi^{-1}(\lambda + L)$ is a flat. Then the function $f$ on $\mathbb{F}_p^n \times \mathbb{F}_p^n$:

$$f(x, y) = x \cdot \pi(y) + \epsilon \phi_{L \perp}(x), \quad (6)$$

where $\epsilon \in \mathbb{F}_p$, is a generalized bent Boolean function.

**Remark**

- The class of bent functions defined as in Equation (6) will be denoted by $\mathcal{C}^p$.
- In general $\mathcal{C}^p$ is not included in the $\mathcal{M}^p$ class.
Existence and nonexistence of $C^p$ I

For construction of $C^p$ class of bent functions, we need a permutation $\pi$ on $\mathbb{F}_p^n$ such that $\pi^{-1}(a + L)$ is a flat for any $a \in \mathbb{F}_p^n$.

**Lemma**

Let $u_1, u_2, u_3 \in \mathbb{F}_3^n$. A set $L = \{u_1, u_2, u_3\}$ is flat of $\mathbb{F}_3^n$ of dimension $\leq 1$ if and only if $u_1 + u_2 + u_3 = 0$.

**Theorem**

Consider the permutation polynomial $\phi$ over $\mathbb{F}_{34}$ [defined by L. Wang],

$$\phi(x) = x^{17} + x.$$

Then there is no 1-dimensional subspace $L$ of $\mathbb{F}_{34}$, such that $\phi(a + L)$ is flat for all $a \in \mathbb{F}_{34}$.
Existence and nonexistence of $CP^{II}$

**Theorem**

Let $\phi$ be a permutation polynomial on $\mathbb{F}_{3^4}$ [defined by L. Wang] of the form

$$\phi(x) = x(x^{16} + 1) = x^{17} + x.$$

Then there is no 2-dimensional subspace $L = \langle u, v \rangle$ such that for all $a \in \mathbb{F}_{3^4}$, $\phi(a + L)$ is flat.

**Remark**

Consider the permutation polynomial [defined by R. Mattews]

$$\phi(x) = x + 1$$

over $\mathbb{F}_{3^4}$. Then for any subspace $L$ of $\mathbb{F}_{3^4}$ with dimension $\leq 2$, $\phi(a + L)$ is flat for all $a \in \mathbb{F}_{3^4}$. 


THANK YOU!