Construction of bent functions based on $\mathbb{Z}$-bent functions

Dr. Sugata Gangopadhyay

Indian Statistical Institute
Chennai Centre

March 21, 2012

Outline

- Introduction to Boolean bent functions.
- Major classes of bent functions.
  - Maiorana–McFarland class.
  - Partial spreads class.
- Bent function construction in a recursive framework by using $\mathbb{Z}$-bent functions. (Dobbertin and Leander [DCC 49 (2008) 3 - 22]).
- Partial spreads type $\mathbb{Z}$-bent functions leading to a new primary construction of bent functons.

Outline

- Introduction to Boolean bent functions.
- Major classes of bent functions.
  - Maiorana–McFarland class.
  - Partial spreads class.
- Bent function construction in a recursive framework by using $\mathbb{Z}$-bent functions. (Dobbertin and Leander [DCC 49 (2008) 3 - 22]).
- Partial spreads type $\mathbb{Z}$-bent functions leading to a new primary construction of bent functons.

Outline

- Introduction to Boolean bent functions.
- Major classes of bent functions.
  - Maiorana–McFarland class.
  - Partial spreads class.
- Bent function construction in a recursive framework by using $\mathbb{Z}$-bent functions. (Dobbertin and Leander [DCC 49 (2008) 3 - 22]).
- Partial spreads type $\mathbb{Z}$-bent functions leading to a new primary construction of bent functons.

Outline

- Introduction to Boolean bent functions.
- Major classes of bent functions.
  - Maiorana–McFarland class.
  - Partial spreads class.
- Bent function construction in a recursive framework by using $\mathbb{Z}$-bent functions. (Dobbertin and Leander [DCC 49 (2008) 3 - 22]).
- Partial spreads type $\mathbb{Z}$-bent functions leading to a new primary construction of bent functons.

Outline

- Introduction to Boolean bent functions.
- Major classes of bent functions.
  - Maiorana–McFarland class.
  - Partial spreads class.
- Bent function construction in a recursive framework by using $\mathbb{Z}$-bent functions. (Dobbertin and Leander [DCC 49 (2008) 3 - 22]).
- Partial spreads type $\mathbb{Z}$-bent functions leading to a new primary construction of bent functons.

Outline

- Introduction to Boolean bent functions.
- Major classes of bent functions.
  - Maiorana–McFarland class.
  - Partial spreads class.
- Bent function construction in a recursive framework by using $\mathbb{Z}$-bent functions. (Dobbertin and Leander [DCC 49 (2008) 3 - 22]).
- Partial spreads type $\mathbb{Z}$-bent functions leading to a new primary construction of bent functons.

Boolean functions

- $\mathbb{F}_2$ is the prime field of characteristic 2.
- $\mathbb{F}_2^n$ is the n dimensional vector space over $\mathbb{F}_2$.
- $\mathbb{F}_{2^n}$ is the n degree extension field of $\mathbb{F}_2$.
- Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables.
- Equivalently any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables.
- The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$.

Boolean functions

- $\mathbb{F}_2$ is the prime field of characteristic 2.
- $\mathbb{F}_2^n$ is the n dimensional vector space over $\mathbb{F}_2$.
- $\mathbb{F}_{2^n}$ is the n degree extension field of $\mathbb{F}_2$.
- Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables.
- Equivalently any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables.
- The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$.

Boolean functions

- $\mathbb{F}_2$ is the prime field of characteristic 2.
- $\mathbb{F}_2^n$ is the n dimensional vector space over $\mathbb{F}_2$.
- $\mathbb{F}_{2^n}$ is the n degree extension field of $\mathbb{F}_2$.
- Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables.
- Equivalently any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables.
- The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$.

Boolean functions

- $\mathbb{F}_2$ is the prime field of characteristic 2.
- $\mathbb{F}_2^n$ is the n dimensional vector space over $\mathbb{F}_2$.
- $\mathbb{F}_{2^n}$ is the n degree extension field of $\mathbb{F}_2$.
- Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables.
- Equivalently any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables.
- The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$.

Boolean functions

- $\mathbb{F}_2$ is the prime field of characteristic 2.
- $\mathbb{F}_2^n$ is the n dimensional vector space over $\mathbb{F}_2$.
- $\mathbb{F}_{2^n}$ is the n degree extension field of $\mathbb{F}_2$.
- Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables.
- Equivalently any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables.
- The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$.

Boolean functions

- $\mathbb{F}_2$ is the prime field of characteristic 2.
- $\mathbb{F}_2^n$ is the n dimensional vector space over $\mathbb{F}_2$.
- $\mathbb{F}_{2^n}$ is the n degree extension field of $\mathbb{F}_2$.
- Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables.
- Equivalently any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables.
- The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$.

The distance between two Boolean functions (1/2)

- The distance between two Boolean functions F and G is

$$\begin{aligned} d_H(F,G) &= \#(F \neq G) \\ &= \frac{1}{2}(\#(F = G) + \#(F \neq G)) \\ &\quad - \frac{1}{2}(\#(F = G) - \#(F \neq G)) \\ &= 2^{n-1} - \frac{1}{2}\sum_{x \in \mathbb{F}_2^n} (-1)^{F(x)+G(x)} \end{aligned} \tag{1}$$

The distance between two Boolean functions (2/2)

- We note that any affine function in $\mathcal{B}_n$ can be written as $\ell_{a,\epsilon}(x) = \langle a, x \rangle + \epsilon$ where $a \in \mathbb{F}_2^n$, $\epsilon \in \mathbb{F}_2$ and $\langle a, x \rangle$ is any inner product of x and a.
-

$$\begin{aligned} d_H(F, \ell_{a,\epsilon}) &= 2^{n-1} - \frac{1}{2} \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x)+\ell_{a,\epsilon}(x)} \\ &= 2^{n-1} - \frac{1}{2} \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x)+\langle a,x \rangle+\epsilon} \\ &= 2^{n-1} - (-1)^{\epsilon} \frac{1}{2} \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x)+\langle a,x \rangle} \end{aligned} \tag{2}$$

The distance between two Boolean functions (2/2)

- We note that any affine function in $\mathcal{B}_n$ can be written as $\ell_{a,\epsilon}(x) = \langle a, x\rangle + \epsilon$ where $a \in \mathbb{F}_2^n$, $\epsilon \in \mathbb{F}_2$ and $\langle a, x\rangle$ is any inner product of x and a.
-

$$\begin{aligned} d_H(F, \ell_{a,\epsilon}) &= 2^{n-1} - \frac{1}{2}\sum_{x\in\mathbb{F}_2^n}(-1)^{F(x)+\ell_{a,\epsilon}(x)} \\ &= 2^{n-1} - \frac{1}{2}\sum_{x\in\mathbb{F}_2^n}(-1)^{F(x)+\langle a,x\rangle+\epsilon} \\ &= 2^{n-1} - (-1)^{\epsilon}\frac{1}{2}\sum_{x\in\mathbb{F}_2^n}(-1)^{F(x)+\langle a,x\rangle} \end{aligned} \tag{2}$$

Walsh–Hadamard transform

- The Walsh–Hadamard transform of F at $a \in \mathbb{F}_2^n$ is

$$W_F(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x)+\langle a,x \rangle}. \tag{3}$$

-

$$\begin{aligned} d_H(F, \ell_{a,\epsilon}) &= 2^{n-1} - (-1)^{\epsilon} \frac{1}{2} \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x)+\langle a,x \rangle} \\ &= 2^{n-1} - (-1)^{\epsilon} \frac{1}{2} W_F(a). \end{aligned} \tag{4}$$

- $\min_{\epsilon \in \mathbb{F}_2}(d_H(f, \ell_{a,\epsilon})) = 2^{n-1} - \frac{1}{2}|W_F(a)|.$

Walsh–Hadamard transform

- The Walsh–Hadamard transform of F at $a \in \mathbb{F}_2^n$ is

$$W_F(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x)+\langle a,x \rangle}. \tag{3}$$

-

$$\begin{aligned} d_H(F, \ell_{a,\epsilon}) &= 2^{n-1} - (-1)^{\epsilon} \frac{1}{2} \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x)+\langle a,x \rangle} \\ &= 2^{n-1} - (-1)^{\epsilon} \frac{1}{2} W_F(a). \end{aligned} \tag{4}$$

- $\min_{\epsilon \in \mathbb{F}_2}(d_H(f, \ell_{a,\epsilon})) = 2^{n-1} - \frac{1}{2}|W_F(a)|$.

Walsh–Hadamard transform

- The Walsh–Hadamard transform of F at $a \in \mathbb{F}_2^n$ is

$$W_F(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x)+\langle a,x \rangle}. \tag{3}$$

-

$$\begin{aligned} d_H(F, \ell_{a,\epsilon}) &= 2^{n-1} - (-1)^{\epsilon} \frac{1}{2} \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x)+\langle a,x \rangle} \\ &= 2^{n-1} - (-1)^{\epsilon} \frac{1}{2} W_F(a). \end{aligned} \tag{4}$$

- $\min_{\epsilon \in \mathbb{F}_2}(d_H(f, \ell_{a,\epsilon})) = 2^{n-1} - \frac{1}{2}|W_F(a)|$.

Nonlinearity

- The nonlinearity of F is defined as:

$$\min_{a \in \mathbb{F}_2^n} \min_{\epsilon \in \mathbb{F}_2}(d_H(F, \ell_{a,\epsilon})) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_F(a)|.$$

- It is known that $\sum_{a \in \mathbb{F}_2^n} W_F(a)^2 = 2^{2n}$. (Parseval's equation).
- Therefore $\max_{a \in \mathbb{F}_2^n} |W_F(a)| \geq 2^{\frac{n}{2}}$ implying that
- nonlinearity of F is bounded above by $2^{n-1} - 2^{\frac{n}{2}-1}$.

Nonlinearity

- The nonlinearity of F is defined as:

$$\min_{a\in\mathbb{F}_2^n}\min_{\epsilon\in\mathbb{F}_2}(d_H(F,\ell_{a,\epsilon})) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}|W_F(a)|.$$

- It is known that $\sum_{a\in\mathbb{F}_2^n} W_F(a)^2 = 2^{2n}$. (Parseval's equation).
- Therefore $\max_{a\in\mathbb{F}_2^n}|W_F(a)| \geq 2^{\frac{n}{2}}$ implying that
- nonlinearity of F is bounded above by $2^{n-1} - 2^{\frac{n}{2}-1}$.

Nonlinearity

- The nonlinearity of F is defined as:

$$\min_{a \in \mathbb{F}_2^n} \min_{\epsilon \in \mathbb{F}_2}(d_H(F, \ell_{a,\epsilon})) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_F(a)|.$$

- It is known that $\sum_{a \in \mathbb{F}_2^n} W_F(a)^2 = 2^{2n}$. (Parseval's equation).
- Therefore $\max_{a \in \mathbb{F}_2^n} |W_F(a)| \geq 2^{\frac{n}{2}}$ implying that
- nonlinearity of F is bounded above by $2^{n-1} - 2^{\frac{n}{2}-1}$.

Nonlinearity

- The nonlinearity of F is defined as:

$$\min_{a \in \mathbb{F}_2^n} \min_{\epsilon \in \mathbb{F}_2}(d_H(F, \ell_{a,\epsilon})) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_F(a)|.$$

- It is known that $\sum_{a \in \mathbb{F}_2^n} W_F(a)^2 = 2^{2n}$. (Parseval's equation).
- Therefore $\max_{a \in \mathbb{F}_2^n} |W_F(a)| \geq 2^{\frac{n}{2}}$ implying that
- nonlinearity of F is bounded above by $2^{n-1} - 2^{\frac{n}{2}-1}$.

Bent functions

- Suppose n is an even positive integer.
- Maximum possible nonlinearity of a Boolean function in $\mathcal{B}_n$ is $2^{n-1} - 2^{\frac{n}{2}-1}$.
- In other words these are the functions for which $W_F(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_2^n$.
- These functions are said to be bent functions.
- Bent functions are Boolean functions which provide maximum resistance to affine approximation.

Bent functions

- Suppose n is an even positive integer.
- Maximum possible nonlinearity of a Boolean function in $\mathcal{B}_n$ is $2^{n-1} - 2^{\frac{n}{2}-1}$.
- In other words these are the functions for which $W_F(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_2^n$.
- These functions are said to be bent functions.
- Bent functions are Boolean functions which provide maximum resistance to affine approximation.

Bent functions

- Suppose n is an even positive integer.
- Maximum possible nonlinearity of a Boolean function in $\mathcal{B}_n$ is $2^{n-1} - 2^{\frac{n}{2}-1}$.
- In other words these are the functions for which $W_F(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_2^n$.
- These functions are said to be bent functions.
- Bent functions are Boolean functions which provide maximum resistance to affine approximation.

Bent functions

- Suppose n is an even positive integer.
- Maximum possible nonlinearity of a Boolean function in $\mathcal{B}_n$ is $2^{n-1} - 2^{\frac{n}{2}-1}$.
- In other words these are the functions for which $W_F(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_2^n$.
- These functions are said to be bent functions.
- Bent functions are Boolean functions which provide maximum resistance to affine approximation.

Bent functions

- Suppose n is an even positive integer.
- Maximum possible nonlinearity of a Boolean function in $\mathcal{B}_n$ is $2^{n-1} - 2^{\frac{n}{2}-1}$.
- In other words these are the functions for which $W_F(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_2^n$.
- These functions are said to be bent functions.
- Bent functions are Boolean functions which provide maximum resistance to affine approximation.

Maiorana–McFarland bent functions (*MMF*): Rothaus 1966

- Let $n = 2k$ and let $F : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be defined as

$$F(y, x) = \langle \pi(y), x \rangle + g(y). \tag{5}$$

where $\pi : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ be a permutation and $G \in \mathcal{B}_k$.

- Rothaus proved that F is a bent function. These are said to be Maiorana–McFarland type bent functions.
- O. Rothaus, *On bent functions*, Journal of Combinatorial Theory, Series A 20 (1976) 300–305.
- O. Rothaus On bent functions, IDA CRD W.P. No. 169. 1966

Maiorana–McFarland bent functions (*MMF*): Rothaus 1966

- Let $n = 2k$ and let $F : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be defined as

$$F(y, x) = \langle \pi(y), x \rangle + g(y). \tag{5}$$

  where $\pi : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ be a permutation and $G \in \mathcal{B}_k$.
- Rothaus proved that F is a bent function. These are said to be Maiorana–McFarland type bent functions.
- O. Rothaus, *On bent functions*, Journal of Combinatorial Theory, Series A 20 (1976) 300–305.
- O. Rothaus On bent functions, IDA CRD W.P. No. 169. 1966

Maiorana–McFarland bent functions (*MMF*): Rothaus 1966

- Let $n = 2k$ and let $F : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be defined as

$$F(y, x) = \langle \pi(y), x \rangle + g(y). \tag{5}$$

  where $\pi : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ be a permutation and $G \in \mathcal{B}_k$.
- Rothaus proved that F is a bent function. These are said to be Maiorana–McFarland type bent functions.
- O. Rothaus, *On bent functions*, Journal of Combinatorial Theory, Series A 20 (1976) 300–305.
- O. Rothaus On bent functions, IDA CRD W.P. No. 169. 1966

Maiorana–McFarland bent functions (*MMF*): Rothaus 1966

- Let $n = 2k$ and let $F : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be defined as

$$F(y, x) = \langle \pi(y), x \rangle + g(y). \tag{5}$$

  where $\pi : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ be a permutation and $G \in \mathcal{B}_k$.
- Rothaus proved that F is a bent function. These are said to be Maiorana–McFarland type bent functions.
- O. Rothaus, *On bent functions*, Journal of Combinatorial Theory, Series A 20 (1976) 300–305.
- O. Rothaus On bent functions, IDA CRD W.P. No. 169. 1966

Partial spreads bent functions: Dillon 1975 (1/2)

- Let $E \subseteq \mathbb{F}_2^n$.

$$\phi_E(x) = \begin{cases} 1 & \text{if } x \in E \\ 0 & \text{if } x \notin E \end{cases}$$

  is the indicator function of E.
- Suppose $\{E_i : i = 1, 2, \cdots, s\}$ is a set of "mutually disjoint" k-dimensional subspaces of $\mathbb{F}_2^n$.
- Here mutually disjoint means $E_i \cap E_j = \{0\}$ whenever $i \neq j$.

Partial spreads bent functions: Dillon 1975 (1/2)

- Let $E \subseteq \mathbb{F}_2^n$.

$$\phi_E(x) = \begin{cases} 1 & \text{if } x \in E \\ 0 & \text{if } x \notin E \end{cases}$$

  is the indicator function of E.

- Suppose $\{E_i : i = 1, 2, \cdots, s\}$ is a set of "mutually disjoint" k-dimensional subspaces of $\mathbb{F}_2^n$.
- Here mutually disjoint means $E_i \cap E_j = \{0\}$ whenever $i \neq j$.

Partial spreads bent functions: Dillon 1975 (1/2)

- Let $E \subseteq \mathbb{F}_2^n$.

$$\phi_E(x) = \begin{cases} 1 & \text{if } x \in E \\ 0 & \text{if } x \notin E \end{cases}$$

  is the indicator function of E.
- Suppose $\{E_i : i = 1, 2, \cdots, s\}$ is a set of "mutually disjoint" k-dimensional subspaces of $\mathbb{F}_2^n$.
- Here mutually disjoint means $E_i \cap E_j = \{0\}$ whenever $i \neq j$.

Partial spreads bent functions: Dillon 1975 (2/2)

- A function $F \in \mathcal{B}_n$ belonging to the class *PS* can be expressed as

$$F(x) = \sum_{i=1}^{s} \phi_{E_i}(x) - 2^{k-1}\phi_{\{0\}}(x) \text{ for all } x \in \mathbb{F}_2^n,$$

  where $s = 2^{k-1}$ if $F \in PS^-$ and $s = 2^{k-1} + 1$ if $F \in PS^+$ and the sum is taken over the integers.

- J. F. Dillon, *Elementary Hadamard difference sets*, Proceedings of Sixth S. E. Conference of Combinatorics, Graph Theory, and Computing, Utility Mathematics, Winnipeg, (1975), 237–249.

Partial spreads bent functions: Dillon 1975 (2/2)

- A function $F \in \mathcal{B}_n$ belonging to the class PS can be expressed as

$$F(x) \quad = \quad \sum_{i=1}^{s} \phi_{E_i}(x) - 2^{k-1}\phi_{\{0\}}(x) \text{ for all } \; x \in \mathbb{F}_2^n,$$

  where $s = 2^{k-1}$ if $F \in PS^-$ and $s = 2^{k-1} + 1$ if $F \in PS^+$ and the sum is taken over the integers.
- J. F. Dillon, *Elementary Hadamard difference sets*, Proceedings of Sixth S. E. Conference of Combinatorics, Graph Theory, and Computing, Utility Mathematics, Winnipeg, (1975), 237–249.

PS_{ap}: an "efficient" construction

- Consider functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.
- Let $V_0 = \mathbb{F}_{2^k}$, the subfield of order 2^k of $\mathbb{F}_{2^n}$.
- Let $V_i = \zeta^i \mathbb{F}_{2^k}$ for all $i = 1, \ldots, 2^k$, where ζ is a primitive element of $\mathbb{F}_{2^n}$.
- The set $\mathcal{S} = \{V_i : i = 0, \ldots, 2^k\}$ consists of mutually disjoint k-dimensional subspaces of $\mathbb{F}_{2^n}$.
- A subclass of *PS* type bent functions, called PS_{ap}, is obtained by constructing functions whose supports are the unions of any 2^{k-1} subspaces belonging to $\mathcal{S}$ excluding 0.
- This subclass of *PS* was originally constructed by Dillon.

PS_{ap}: an "efficient" construction

- Consider functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.
- Let $V_0 = \mathbb{F}_{2^k}$, the subfield of order 2^k of $\mathbb{F}_{2^n}$.
- Let $V_i = \zeta^i \mathbb{F}_{2^k}$ for all $i = 1, \ldots, 2^k$, where ζ is a primitive element of $\mathbb{F}_{2^n}$.
- The set $\mathcal{S} = \{V_i : i = 0, \ldots, 2^k\}$ consists of mutually disjoint k-dimensional subspaces of $\mathbb{F}_{2^n}$.
- A subclass of *PS* type bent functions, called PS_{ap}, is obtained by constructing functions whose supports are the unions of any 2^{k-1} subspaces belonging to $\mathcal{S}$ excluding 0.
- This subclass of *PS* was originally constructed by Dillon.

PS_{ap}: an "efficient" construction

- Consider functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.
- Let $V_0 = \mathbb{F}_{2^k}$, the subfield of order 2^k of $\mathbb{F}_{2^n}$.
- Let $V_i = \zeta^i \mathbb{F}_{2^k}$ for all $i = 1, \ldots, 2^k$, where ζ is a primitive element of $\mathbb{F}_{2^n}$.
- The set $\mathcal{S} = \{V_i : i = 0, \ldots, 2^k\}$ consists of mutually disjoint k-dimensional subspaces of $\mathbb{F}_{2^n}$.
- A subclass of PS type bent functions, called PS_{ap}, is obtained by constructing functions whose supports are the unions of any 2^{k-1} subspaces belonging to $\mathcal{S}$ excluding 0.
- This subclass of PS was originally constructed by Dillon.

PS_{ap}: an "efficient" construction

- Consider functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.
- Let $V_0 = \mathbb{F}_{2^k}$, the subfield of order 2^k of $\mathbb{F}_{2^n}$.
- Let $V_i = \zeta^i \mathbb{F}_{2^k}$ for all $i = 1, \ldots, 2^k$, where ζ is a primitive element of $\mathbb{F}_{2^n}$.
- The set $\mathcal{S} = \{ V_i : i = 0, \ldots, 2^k \}$ consists of mutually disjoint k-dimensional subspaces of $\mathbb{F}_{2^n}$.
- A subclass of *PS* type bent functions, called PS_{ap}, is obtained by constructing functions whose supports are the unions of any 2^{k-1} subspaces belonging to $\mathcal{S}$ excluding 0.
- This subclass of *PS* was originally constructed by Dillon.

PS_{ap}: an "efficient" construction

- Consider functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.
- Let $V_0 = \mathbb{F}_{2^k}$, the subfield of order 2^k of $\mathbb{F}_{2^n}$.
- Let $V_i = \zeta^i \mathbb{F}_{2^k}$ for all $i = 1, \ldots, 2^k$, where ζ is a primitive element of $\mathbb{F}_{2^n}$.
- The set $\mathcal{S} = \{V_i : i = 0, \ldots, 2^k\}$ consists of mutually disjoint k-dimensional subspaces of $\mathbb{F}_{2^n}$.
- A subclass of *PS* type bent functions, called PS_{ap}, is obtained by constructing functions whose supports are the unions of any 2^{k-1} subspaces belonging to $\mathcal{S}$ excluding 0.
- This subclass of *PS* was originally constructed by Dillon.

PS_{ap}: an "efficient" construction

- Consider functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.
- Let $V_0 = \mathbb{F}_{2^k}$, the subfield of order 2^k of $\mathbb{F}_{2^n}$.
- Let $V_i = \zeta^i \mathbb{F}_{2^k}$ for all $i = 1, \ldots, 2^k$, where ζ is a primitive element of $\mathbb{F}_{2^n}$.
- The set $\mathcal{S} = \{V_i : i = 0, \ldots, 2^k\}$ consists of mutually disjoint k-dimensional subspaces of $\mathbb{F}_{2^n}$.
- A subclass of *PS* type bent functions, called PS_{ap}, is obtained by constructing functions whose supports are the unions of any 2^{k-1} subspaces belonging to $\mathcal{S}$ excluding 0.
- This subclass of *PS* was originally constructed by Dillon.

Other Classes of bent functions: Carlet 1993, Dobertin et al. 2006

- Carlet modified *MMF* and *PS* type bent functions to construct *two new classes of bent functions*. (Eurocrypt '93, LNCS, Vol. 765, (1994), pp. 77–101).
- Bent functions via Kasami exponents. (Dobbertin and Leander, *A survey of some recent results on bent functions*, SETA 2004, LNCS 3486.)
- H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke and P. Gaborit, *Construction of bent functions via Niho power functions*, Journal of Combinatorial Theory, Series A, 113 (2006), 779–798.
- Carlet and Mesnager, *On Dillon's class H of bent functions, Niho bent functions and o-polynomials*, Journal of Combinatorial Theory, Series A, 118 (2011) 2392–2410.

Other Classes of bent functions: Carlet 1993, Dobertin et al. 2006

- Carlet modified *MMF* and *PS* type bent functions to construct *two new classes of bent functions*. (Eurocrypt '93, LNCS, Vol. 765, (1994), pp. 77–101).
- Bent functions via Kasami exponents. (Dobbertin and Leander, *A survey of some recent results on bent functions*, SETA 2004, LNCS 3486.)
- H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke and P. Gaborit, *Construction of bent functions via Niho power functions*, Journal of Combinatorial Theory, Series A, 113 (2006), 779–798.
- Carlet and Mesnager, *On Dillon's class H of bent functions, Niho bent functions and o-polynomials*, Journal of Combinatorial Theory, Series A, 118 (2011) 2392–2410.

Other Classes of bent functions: Carlet 1993, Dobertin et al. 2006

- Carlet modified *MMF* and *PS* type bent functions to construct *two new classes of bent functions*. (Eurocrypt '93, LNCS, Vol. 765, (1994), pp. 77–101).
- Bent functions via Kasami exponents. (Dobbertin and Leander, *A survey of some recent results on bent functions*, SETA 2004, LNCS 3486.)
- H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke and P. Gaborit, *Construction of bent functions via Niho power functions*, Journal of Combinatorial Theory, Series A, 113 (2006), 779–798.
- Carlet and Mesnager, *On Dillon's class H of bent functions, Niho bent functions and o-polynomials*, Journal of Combinatorial Theory, Series A, 118 (2011) 2392–2410.

Other Classes of bent functions: Carlet 1993, Dobertin et al. 2006

- Carlet modified *MMF* and *PS* type bent functions to construct *two new classes of bent functions*. (Eurocrypt '93, LNCS, Vol. 765, (1994), pp. 77–101).
- Bent functions via Kasami exponents. (Dobbertin and Leander, *A survey of some recent results on bent functions*, SETA 2004, LNCS 3486.)
- H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke and P. Gaborit, *Construction of bent functions via Niho power functions*, Journal of Combinatorial Theory, Series A, 113 (2006), 779–798.
- Carlet and Mesnager, *On Dillon's class H of bent functions, Niho bent functions and o-polynomials*, Journal of Combinatorial Theory, Series A, 118 (2011) 2392–2410.

Quoting Dobberin and Leander: 2008 DCC

- "A main obstacle in the study of bent functions is the lack of recurrence laws. There are only few constructions deriving bent functions from smaller ones. But it seems that most bent functions appear without any roots to bent functions in lower dimensions, which could explain their existence."
- Dobbertin and Leander (2008 DCC) did exactly that but they had to go out of the class of bent functions to $\mathbb{Z}$-bent functions.
- In fact, they went out of the class of Boolean functions.
- H. Dobbertin, G. Leander, *Bent functions embedded into the recursive framework of $\mathbb{Z}$-bent functions*, Des. Codes Cryptogr. 49 (2008), 3–22.

Quoting Dobberin and Leander: 2008 DCC

- "A main obstacle in the study of bent functions is the lack of recurrence laws. There are only few constructions deriving bent functions from smaller ones. But it seems that most bent functions appear without any roots to bent functions in lower dimensions, which could explain their existence."
- Dobbertin and Leander (2008 DCC) did exactly that but they had to go out of the class of bent functions to $\mathbb{Z}$-bent functions.
- In fact, they went out of the class of Boolean functions.
- H. Dobbertin, G. Leander, *Bent functions embedded into the recursive framework of $\mathbb{Z}$-bent functions*, Des. Codes Cryptogr. 49 (2008), 3–22.

Quoting Dobberin and Leander: 2008 DCC

- "A main obstacle in the study of bent functions is the lack of recurrence laws. There are only few constructions deriving bent functions from smaller ones. But it seems that most bent functions appear without any roots to bent functions in lower dimensions, which could explain their existence."
- Dobbertin and Leander (2008 DCC) did exactly that but they had to go out of the class of bent functions to $\mathbb{Z}$-bent functions.
- In fact, they went out of the class of Boolean functions.
- H. Dobbertin, G. Leander, *Bent functions embedded into the recursive framework of $\mathbb{Z}$-bent functions*, Des. Codes Cryptogr. 49 (2008), 3–22.

Quoting Dobberin and Leander: 2008 DCC

- “A main obstacle in the study of bent functions is the lack of recurrence laws. There are only few constructions deriving bent functions from smaller ones. But it seems that most bent functions appear without any roots to bent functions in lower dimensions, which could explain their existence.”
- Dobbertin and Leander (2008 DCC) did exactly that but they had to go out of the class of bent functions to $\mathbb{Z}$-bent functions.
- In fact, they went out of the class of Boolean functions.
- H. Dobbertin, G. Leander, *Bent functions embedded into the recursive framework of $\mathbb{Z}$-bent functions*, Des. Codes Cryptogr. 49 (2008), 3–22.

$\mathbb{Z}$-bent functions (1/2)

- Given a Boolean function F we consider the function

$$\begin{aligned} f : \mathbb{F}_2^n &\rightarrow \{-1, 1\} \subseteq \mathbb{Z} \text{ defined by} \\ f(x) &= (-1)^{F(x)} \text{ for all } x \in \mathbb{F}_2^n. \end{aligned}$$

- The *Fourier transform* defined by

$$\hat{f}(a) = \frac{1}{2^k} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\langle a,x \rangle}.$$

- The Walsh-transform given by $\hat{f}(a) = \frac{1}{2^k} W_F(a)$.
- f is bent if and only if both f and $\hat{f}$ are $\{-1, 1\}$-valued.
- f is said to be $\mathbb{Z}$-bent of level 0.

$\mathbb{Z}$-bent functions (1/2)

- Given a Boolean function F we consider the function

$$\begin{array}{rcl} f : \mathbb{F}_2^n & \to & \{-1, 1\} \subseteq \mathbb{Z} \text{ defined by} \\ f(x) & = & (-1)^{F(x)} \text{ for all } x \in \mathbb{F}_2^n. \end{array}$$

- The *Fourier transform* defined by

$$\hat{f}(a) = \frac{1}{2^k} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\langle a,x \rangle}.$$

- The Walsh-transform given by $\hat{f}(a) = \frac{1}{2^k} W_F(a)$.
- f is bent if and only if both f and $\hat{f}$ are $\{-1, 1\}$-valued.
- f is said to be $\mathbb{Z}$-bent of level 0.

$\mathbb{Z}$-bent functions (1/2)

- Given a Boolean function F we consider the function

$$\begin{aligned} f : \mathbb{F}_2^n &\rightarrow \{-1, 1\} \subseteq \mathbb{Z} \text{ defined by} \\ f(x) &= (-1)^{F(x)} \text{ for all } x \in \mathbb{F}_2^n. \end{aligned}$$

- The *Fourier transform* defined by

$$\hat{f}(a) = \frac{1}{2^k} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\langle a,x \rangle}.$$

- The Walsh-transform given by $\hat{f}(a) = \frac{1}{2^k} W_F(a)$.
- f is bent if and only if both f and $\hat{f}$ are $\{-1, 1\}$-valued.
- f is said to be $\mathbb{Z}$-bent of level 0.

$\mathbb{Z}$-bent functions (1/2)

- Given a Boolean function F we consider the function

$$\begin{aligned} f : \mathbb{F}_2^n &\rightarrow \{-1, 1\} \subseteq \mathbb{Z} \text{ defined by} \\ f(x) &= (-1)^{F(x)} \text{ for all } x \in \mathbb{F}_2^n. \end{aligned}$$

- The *Fourier transform* defined by

$$\hat{f}(a) = \frac{1}{2^k} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\langle a,x \rangle}.$$

- The Walsh-transform given by $\hat{f}(a) = \frac{1}{2^k} W_F(a)$.
- f is bent if and only if both f and $\hat{f}$ are $\{-1, 1\}$-valued.
- f is said to be $\mathbb{Z}$-bent of level 0.

$\mathbb{Z}$-bent functions (1/2)

- Given a Boolean function F we consider the function

$$\begin{aligned} f : \mathbb{F}_2^n &\rightarrow \{-1, 1\} \subseteq \mathbb{Z} \text{ defined by} \\ f(x) &= (-1)^{F(x)} \text{ for all } x \in \mathbb{F}_2^n. \end{aligned}$$

- The *Fourier transform* defined by

$$\hat{f}(a) = \frac{1}{2^k} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\langle a,x \rangle}.$$

- The Walsh-transform given by $\hat{f}(a) = \frac{1}{2^k} W_F(a)$.
- f is bent if and only if both f and $\hat{f}$ are $\{-1, 1\}$-valued.
- f is said to be $\mathbb{Z}$-bent of level 0.

$\mathbb{Z}$-bent functions (2/2)

- $$\begin{aligned} W_0 &= \{-1, 1\}, \\ W_r &= \{w \in \mathbb{Z} | -2^{r-1} \le w \le 2^{r-1}\} \text{ for } r > 0. \end{aligned}$$
- A function $f : \mathbb{F}_2^n \longrightarrow W_r$ is said to be a $\mathbb{Z}$-bent function of *size* k (equivalently, on n variables) and *level* r if and only if $\hat{f}$ is also a function into W_r. The set of all $\mathbb{Z}$-bent functions of size k and level r is denoted by $\mathcal{B}F_r^k$.
- Any function belonging to $\cup_{r \ge 0} \mathcal{B}F_r^k$ is said to be a $\mathbb{Z}$-bent function.

$\mathbb{Z}$-bent functions (2/2)

-

$$\begin{aligned} W_0 &= \{-1, 1\}, \\ W_r &= \{w \in \mathbb{Z} | -2^{r-1} \leq w \leq 2^{r-1}\} \text{ for } r > 0. \end{aligned}$$

- A function $f : \mathbb{F}_2^n \longrightarrow W_r$ is said to be a $\mathbb{Z}$-bent function of *size* k (equivalently, on n variables) and *level* r if and only if $\hat{f}$ is also a function into W_r. The set of all $\mathbb{Z}$-bent functions of size k and level r is denoted by $\mathcal{B}F_r^k$.
- Any function belonging to $\cup_{r\geq 0}\mathcal{B}F_r^k$ is said to be a $\mathbb{Z}$-bent function.

$\mathbb{Z}$-bent functions (2/2)

- $$\begin{aligned} W_0 &= \{-1, 1\}, \\ W_r &= \{w \in \mathbb{Z} | -2^{r-1} \leq w \leq 2^{r-1}\} \text{ for } r > 0. \end{aligned}$$
- A function $f : \mathbb{F}_2^n \longrightarrow W_r$ is said to be a $\mathbb{Z}$-bent function of *size* k (equivalently, on n variables) and *level* r if and only if $\hat{f}$ is also a function into W_r. The set of all $\mathbb{Z}$-bent functions of size k and level r is denoted by $\mathcal{B}F_r^k$.
- Any function belonging to $\cup_{r \geq 0} \mathcal{B}F_r^k$ is said to be a $\mathbb{Z}$-bent function.

From bent to $\mathbb{Z}$-bent functions and back (1/3)

- Suppose $f \in \mathcal{B}F_r^k$, and

$$h_{\epsilon_1\epsilon_2}(y) = f(\epsilon_1, \epsilon_2, y), \text{ for all } (\epsilon_1, \epsilon_2, y) \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^{n-2}.$$

Define functions $f_{\epsilon_1\epsilon_2}$ as follows:

- For $r = 0$:

$$\begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix}. \quad (6)$$

- For $r \geq 1$:

$$\begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix}. \quad (7)$$

From bent to $\mathbb{Z}$-bent functions and back (1/3)

- Suppose $f \in \mathcal{B}F_r^k$, and

$$h_{\epsilon_1\epsilon_2}(y) = f(\epsilon_1, \epsilon_2, y), \text{ for all } (\epsilon_1, \epsilon_2, y) \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^{n-2}.$$

  Define functions $f_{\epsilon_1\epsilon_2}$ as follows:

- For $r = 0$:

$$\begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix}. \quad (6)$$

- For $r \geq 1$:

$$\begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix}. \quad (7)$$

From bent to $\mathbb{Z}$-bent functions and back (1/3)

- Suppose $f \in \mathcal{B}F_r^k$, and

$$h_{\epsilon_1\epsilon_2}(y) = f(\epsilon_1, \epsilon_2, y), \text{ for all } (\epsilon_1, \epsilon_2, y) \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^{n-2}.$$

  Define functions $f_{\epsilon_1\epsilon_2}$ as follows:
- For $r = 0$:

$$\begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix}. \quad (6)$$

- For $r \geq 1$:

$$\begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix}. \quad (7)$$

From bent to $\mathbb{Z}$-bent functions and back (2/3)

- Dobbertin and Leander proved that if f is a $\mathbb{Z}$-bent function of size k level r then $f_{\epsilon_1,\epsilon_2}$ are $\mathbb{Z}$-bent functions of size $k-1$ and level $r+1$.
- Thus all $\mathbb{Z}$-bent functions of size k and level r are obtained by "gluing" $\mathbb{Z}$-bent functions of size $k-1$ and level $r+1$.
- The "gluing" process is described in the next slide.

From bent to $\mathbb{Z}$-bent functions and back (2/3)

- Dobbertin and Leander proved that if f is a $\mathbb{Z}$-bent function of size k level r then $f_{\epsilon_1,\epsilon_2}$ are $\mathbb{Z}$-bent functions of size $k-1$ and level $r+1$.
- Thus all $\mathbb{Z}$-bent functions of size k and level r are obtained by "gluing" $\mathbb{Z}$-bent functions of size $k-1$ and level $r+1$.
- The "gluing" process is described in the next slide.

From bent to $\mathbb{Z}$-bent functions and back (2/3)

- Dobbertin and Leander proved that if f is a $\mathbb{Z}$-bent function of size k level r then $f_{\epsilon_1,\epsilon_2}$ are $\mathbb{Z}$-bent functions of size $k-1$ and level $r+1$.
- Thus all $\mathbb{Z}$-bent functions of size k and level r are obtained by "gluing" $\mathbb{Z}$-bent functions of size $k-1$ and level $r+1$.
- The "gluing" process is described in the next slide.

From bent to $\mathbb{Z}$-bent functions and back (3/3)

- The gluing process.
- For $r = 0$:

$$\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix}. \tag{8}$$

- For $r \geq 1$:

$$\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix}. \tag{9}$$

From bent to $\mathbb{Z}$-bent functions and back (3/3)

- The gluing process.
- For $r = 0$:

$$\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix}. \tag{8}$$

- For $r \geq 1$:

$$\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix}. \tag{9}$$

From bent to $\mathbb{Z}$-bent functions and back (3/3)

- The gluing process.
- For $r = 0$:

$$\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix}. \tag{8}$$

- For $r \geq 1$:

$$\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix}. \tag{9}$$

A construction of $\mathbb{Z}$-bent functions of arbitrary level (1/2)

- Let $m_1, m_2, \cdots, m_s \in \mathbb{Z}$ and $E_1, E_2, \cdots, E_s$ be k-dimensional subspaces of $\mathbb{F}_2^n$, then the function

$$f(x) = \sum_{i=1}^{s} m_i \phi_{E_i}(x)$$

is a $\mathbb{Z}$-bent function and its dual is given by $\sum_{i=1}^{s} m_i \phi_{E_i^\perp}(x)$.

A construction of $\mathbb{Z}$-bent functions of arbitrary level (2/2)

- Suppose $\{E_i : i = 1, 2, \cdots, s\}$ is a set of k-dimensional subspaces of $\mathbb{F}_2^n$ with the property that $E_i \cap E_j = \{0\}$ whenever $i \neq j$. The function

$$f(x) = \sum_{i=1}^{s} m_i \phi_{E_i}(x), \text{ for all } x \in \mathbb{F}_2^n, \tag{10}$$

where $m_i \in W_r$, for all $i = 1, 2, \ldots, s$, is a $\mathbb{Z}$-bent function of level r, for any $r \geq 1$, if and only if $\sum_{i=1}^{s} m_i \in W_r$.

Proof Outline

- $$\begin{aligned}
\hat{f}(a) &= \frac{1}{2^k}\sum_{x\in\mathbb{F}_2^n} f(x)(-1)^{\langle a,x\rangle} \\
&= \frac{1}{2^k}\sum_{x\in\mathbb{F}_2^n}\sum_{i=1}^{s} m_i\phi_{E_i}(x)(-1)^{\langle a,x\rangle} \\
&= \frac{1}{2^k}\sum_{i=1}^{s} m_i\sum_{x\in E_i}(-1)^{\langle a,x\rangle} \\
&= \frac{1}{2^k}\sum_{i=1}^{s} m_i 2^k\phi_{E_i^\perp}(a) \\
&= \sum_{i=1}^{s} m_i\phi_{E_i^\perp}(a)
\end{aligned}$$

A new primary construction of bent functions (1/5)

- Let four $\mathbb{Z}$-bent functions $f_{00}, f_{01}, f_{10}, f_{11}$ of level 1 and size k be given such that

$$\begin{aligned} f_{00}(x) &\equiv f_{01}(x) + 1 \bmod 2, && (11)\\ f_{10}(x) &\equiv f_{11}(x) + 1 \bmod 2, && (12)\\ \hat{f}_{00}(x) &\equiv \hat{f}_{10}(x) + 1 \bmod 2, && (13)\\ \hat{f}_{01}(x) &\equiv \hat{f}_{11}(x) + 1 \bmod 2. && (14) \end{aligned}$$

  Then the function

$$\begin{aligned} h : \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^n &\rightarrow \{-1, 1\} \text{ defined by} \\ h(y, z, x) &= h_{yz}(x) \text{ for all } x \in \mathbb{F}_2^n, \end{aligned}$$

  where

$$\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix}$$

  is a bent function (of level 0).

A new primary construction of bent functions (2/5)

- We start by letting $\mathcal{S} = \{S_i\}$ be a spread, i.e. a collection of $2^k + 1$ subspaces of dimension k with the condition that

$$S_i \cap S_j = \{0\} \text{ for } i \neq j, \text{ and } \cup_i S_i = \mathbb{F}_2^n.$$

- Next, we partition this spread $\mathcal{S}$ into two parts, $\mathcal{A}$ and $\mathcal{B}$, i.e. $\mathcal{A} \cap \mathcal{B} = \emptyset$ and $\mathcal{A} \cup \mathcal{B} = \mathcal{S}$ and select coefficients, $m_A, m'_A, n_B, n'_B \in \{-1, 1\}$ for all $A \in \mathcal{A}$ and $B \in \mathcal{B}$,

$$\begin{array}{lll} (m_A)_{A\in\mathcal{A}} & \text{such that} & \sum m_A \in \{-1,0,1\}, \\ (m'_A)_{A\in\mathcal{A}} & \text{such that} & \sum m'_A \in \{-1,0,1\}, \\ (n_B)_{B\in\mathcal{B}} & \text{such that} & \sum n_B \in \{-1,0,1\}, \\ (n'_B)_{B\in\mathcal{B}} & \text{such that} & \sum n'_B \in \{-1,0,1\}. \end{array}$$

A new primary construction of bent functions (2/5)

- We start by letting $\mathcal{S} = \{S_i\}$ be a spread, i.e. a collection of $2^k + 1$ subspaces of dimension k with the condition that

$$S_i \cap S_j = \{0\} \text{ for } i \neq j, \text{ and } \cup_i S_i = \mathbb{F}_2^n.$$

- Next, we partition this spread $\mathcal{S}$ into two parts, $\mathcal{A}$ and $\mathcal{B}$, i.e. $\mathcal{A} \cap \mathcal{B} = \emptyset$ and $\mathcal{A} \cup \mathcal{B} = \mathcal{S}$ and select coefficients, $m_A, m'_A, n_B, n'_B \in \{-1, 1\}$ for all $A \in \mathcal{A}$ and $B \in \mathcal{B}$,

$$\begin{aligned}
(m_A)_{A\in\mathcal{A}} &\quad \text{such that} \quad \sum m_A \in \{-1, 0, 1\}, \\
(m'_A)_{A\in\mathcal{A}} &\quad \text{such that} \quad \sum m'_A \in \{-1, 0, 1\}, \\
(n_B)_{B\in\mathcal{B}} &\quad \text{such that} \quad \sum n_B \in \{-1, 0, 1\}, \\
(n'_B)_{B\in\mathcal{B}} &\quad \text{such that} \quad \sum n'_B \in \{-1, 0, 1\}.
\end{aligned}$$

A new primary construction of bent functions (3/5)

- Construct

$$
\begin{aligned}
f_{00}(x) &= \sum_{A \in \mathcal{A}} m_A \phi_A(x), \\
f_{10}(x) &= \sum_{B \in \mathcal{B}} n_B \phi_B(x), \\
f_{01}(x) &= \sum_{B \in \mathcal{B}} n'_B \phi_B(x), \\
f_{11}(x) &= \sum_{A \in \mathcal{A}} m'_A \phi_A(x).
\end{aligned}
$$

A new primary construction of bent functions (4/5)

- If $x \in \mathbb{F}_2^n$, then

$$\begin{aligned} f_{00}(x) + f_{01}(x) &= \sum_{A \in \mathcal{A}} m_A \phi_A(x) + \sum_{B \in \mathcal{B}} n'_B \phi_B(x) \\ &= \sum_{A \in \mathcal{A}} \phi_A(x) + \sum_{B \in \mathcal{B}} \phi_B(x) \pmod 2 \\ &= \sum_{S_i \in \mathcal{S}} \phi_{S_i}(x) \pmod 2. \end{aligned}$$

- If $x \neq 0$ then, as $\mathcal{S}$ is a spread, there exists exactly one subspace S_k such that $x \in S_k$ and

$$f_{00}(x) + f_{01}(x) = \sum_{S_i \in \mathcal{S}} \phi_{S_i}(x) = \phi_{S_k}(x) = 1 \pmod 2.$$

On the other hand, if $x = 0$ then

$$f_{00}(0) + f_{01}(0) = \sum_{S_i \in \mathcal{S}} 1 = 2^k + 1 = 1 \pmod 2.$$

A new primary construction of bent functions (4/5)

- If $x \in \mathbb{F}_2^n$, then

$$\begin{aligned} f_{00}(x) + f_{01}(x) &= \sum_{A \in \mathcal{A}} m_A \phi_A(x) + \sum_{B \in \mathcal{B}} n'_B \phi_B(x) \\ &= \sum_{A \in \mathcal{A}} \phi_A(x) + \sum_{B \in \mathcal{B}} \phi_B(x) \pmod 2 \\ &= \sum_{S_i \in \mathcal{S}} \phi_{S_i}(x) \pmod 2. \end{aligned}$$

- If $x \neq 0$ then, as $\mathcal{S}$ is a spread, there exists exactly one subspace S_k such that $x \in S_k$ and

$$f_{00}(x) + f_{01}(x) = \sum_{S_i \in \mathcal{S}} \phi_{S_i}(x) = \phi_{S_k}(x) = 1 \pmod 2.$$

  On the other hand, if $x = 0$ then

$$f_{00}(0) + f_{01}(0) = \sum_{S_i \in \mathcal{S}} 1 = 2^k + 1 = 1 \pmod 2.$$

A new primary construction of bent functions (5/5)

- We compute

$$
\begin{aligned}
h_{00} &= f_{00} + f_{01}, \\
h_{01} &= f_{00} - f_{01}, \\
h_{10} &= f_{01} + f_{11}, \\
h_{11} &= f_{01} - f_{11}.
\end{aligned}
$$

- The gives a bent function.

A new primary construction of bent functions (5/5)

- We compute

$$\begin{aligned} h_{00} &= f_{00} + f_{01}, \\ h_{01} &= f_{00} - f_{01}, \\ h_{10} &= f_{01} + f_{11}, \\ h_{11} &= f_{01} - f_{11}. \end{aligned}$$

- The gives a bent function.

Construction of an 8-variable bent function (1/2)

- Let ζ be a root of the primitive polynomial $x^6 + x + 1$ on $\mathbb{F}_2$. We consider the finite field $\mathbb{F}_{2^6} = \{\zeta^i : i = 0, 1, \ldots, 62\} \cup \{0\}$.
- The subfield $V_0 = \mathbb{F}_{2^3} = \{\zeta^{9i} : i = 0, 1, \ldots, 6\} \cup \{0\}$, along with the spread

$$\mathcal{S} = \{V_i : V_i = \zeta^i V_0, i = 0, 1, \ldots, 8\}.$$

- The subsets $\mathcal{A} = \{V_0, V_1, V_2, V_3, V_4\}$ and $\mathcal{B} = \{V_5, V_6, V_7, V_8\}$ form a partition of $\mathcal{S}$.

Construction of an 8-variable bent function (1/2)

- Let ζ be a root of the primitive polynomial $x^6 + x + 1$ on $\mathbb{F}_2$. We consider the finite field $\mathbb{F}_{2^6} = \{\zeta^i : i = 0, 1, \ldots, 62\} \cup \{0\}$.
- The subfield $V_0 = \mathbb{F}_{2^3} = \{\zeta^{9i} : i = 0, 1, \ldots, 6\} \cup \{0\}$, along with the spread

$$\mathcal{S} = \{V_i : V_i = \zeta^i V_0, i = 0, 1, \ldots, 8\}.$$

- The subsets $\mathcal{A} = \{V_0, V_1, V_2, V_3, V_4\}$ and $\mathcal{B} = \{V_5, V_6, V_7, V_8\}$ form a partition of $\mathcal{S}$.

Construction of an 8-variable bent function (1/2)

- Let ζ be a root of the primitive polynomial $x^6 + x + 1$ on $\mathbb{F}_2$. We consider the finite field $\mathbb{F}_{2^6} = \{\zeta^i : i = 0, 1, \ldots, 62\} \cup \{0\}$.
- The subfield $V_0 = \mathbb{F}_{2^3} = \{\zeta^{9i} : i = 0, 1, \ldots, 6\} \cup \{0\}$, along with the spread

$$\mathcal{S} = \{V_i : V_i = \zeta^i V_0, i = 0, 1, \ldots, 8\}.$$

- The subsets $\mathcal{A} = \{V_0, V_1, V_2, V_3, V_4\}$ and $\mathcal{B} = \{V_5, V_6, V_7, V_8\}$ form a partition of $\mathcal{S}$.

Construction of an 8-variable bent function (2/2)

- Consider the following four $\mathbb{Z}$-bent function of level 1.

$$\begin{aligned} f_{00}(x) &= \phi_{V_0}(x) - \phi_{V_1}(x) + \phi_{V_2}(x) - \phi_{V_3}(x) + \phi_{V_4}(x), \\ f_{10}(x) &= \phi_{V_5}(x) - \phi_{V_6}(x) - \phi_{V_7}(x) + \phi_{V_8}(x), \\ f_{01}(x) &= \phi_{V_5}(x) - \phi_{V_6}(x) + \phi_{V_7}(x) - \phi_{V_8}(x), \\ f_{11}(x) &= \phi_{V_0}(x) + \phi_{V_1}(x) - \phi_{V_2}(x) - \phi_{V_3}(x) - \phi_{V_4}(x). \end{aligned}$$

- We construct $h_{00} = f_{00} + f_{01}$, $h_{01} = f_{00} - f_{01}$, $h_{10} = f_{10} + f_{11}$ and $h_{11} = f_{10} - f_{11}$. The 8-variable function

$$\begin{aligned} f(y,z,x) &= (1+y)(1+z)h_{00}(x) + (1+y)zh_{01}(x) \\ &\quad + y(1+z)h_{10}(x) + yzh_{11}(x), \\ &\quad \text{for all } (y,z,x) \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_{2^6}, \end{aligned}$$

is bent.

Construction of an 8-variable bent function (2/2)

- Consider the following four $\mathbb{Z}$-bent function of level 1.

$$\begin{aligned}
f_{00}(x) &= \phi_{V_0}(x) - \phi_{V_1}(x) + \phi_{V_2}(x) - \phi_{V_3}(x) + \phi_{V_4}(x),\\
f_{10}(x) &= \phi_{V_5}(x) - \phi_{V_6}(x) - \phi_{V_7}(x) + \phi_{V_8}(x),\\
f_{01}(x) &= \phi_{V_5}(x) - \phi_{V_6}(x) + \phi_{V_7}(x) - \phi_{V_8}(x),\\
f_{11}(x) &= \phi_{V_0}(x) + \phi_{V_1}(x) - \phi_{V_2}(x) - \phi_{V_3}(x) - \phi_{V_4}(x).
\end{aligned}$$

- We construct $h_{00} = f_{00} + f_{01}$, $h_{01} = f_{00} - f_{01}$, $h_{10} = f_{10} + f_{11}$ and $h_{11} = f_{10} - f_{11}$. The 8-variable function

$$\begin{aligned}
f(y,z,x) &= (1+y)(1+z)h_{00}(x) + (1+y)zh_{01}(x)\\
&\quad + y(1+z)h_{10}(x) + yzh_{11}(x),\\
&\quad \text{for all } (y,z,x) \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_{2^6},
\end{aligned}$$

  is bent.

Checking (affine) inequivalence

- Two Boolean functions F and G are equivalent if and only if there exists $A \in GL(n, \mathbb{F}_2)$ and $b, u \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$ such that
$$G(x) = F(Ax + b) + \langle u, x \rangle + \epsilon.$$
- The second-derivative of F at a subspace V generated by $a, b \in \mathbb{F}_2^n$, $a \neq b$ is defined as
$$D_V F(x) = F(x) + F(x + a) + F(x + b) + F(x + a + b).$$
- The frequency distribution of the weights of the second-derivatives of F with respect to all the distinct two-dimensional subspaces of $\mathbb{F}_{2^8}$ is

Weights	64	96	112	128	144	160	256
# of subspaces	56	224	2240	5810	1344	1120	1

Checking (affine) inequivalence

- Two Boolean functions F and G are equivalent if and only if there exists $A \in GL(n, \mathbb{F}_2)$ and $b, u \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$ such that
$$G(x) = F(Ax + b) + \langle u, x \rangle + \epsilon.$$
- The second-derivative of F at a subspace V generated by $a, b \in \mathbb{F}_2^n$, $a \neq b$ is defined as
$$D_V F(x) = F(x) + F(x + a) + F(x + b) + F(x + a + b).$$
- The frequency distribution of the weights of the second-derivatives of F with respect to all the distinct two-dimensional subspaces of $\mathbb{F}_{2^8}$ is

Weights	64	96	112	128	144	160	256
# of subspaces	56	224	2240	5810	1344	1120	1

Checking (affine) inequivalence

- Two Boolean functions F and G are equivalent if and only if there exists $A \in GL(n, \mathbb{F}_2)$ and $b, u \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$ such that
$$G(x) = F(Ax + b) + \langle u, x \rangle + \epsilon.$$
- The second-derivative of F at a subspace V generated by $a, b \in \mathbb{F}_2^n$, $a \neq b$ is defined as
$$D_V F(x) = F(x) + F(x + a) + F(x + b) + F(x + a + b).$$
- The frequency distribution of the weights of the second-derivatives of F with respect to all the distinct two-dimensional subspaces of $\mathbb{F}_{2^8}$ is

Weights	64	96	112	128	144	160	256
# of subspaces	56	224	2240	5810	1344	1120	1

Classes of inequivalent PS_{ap} bents on 8-variables

0	64	96	112	128	144	160	192	# of functions
0	0	940	2360	3885	2360	1220	30	8160
0	75	605	1760	5640	1600	1055	60	4080
0	0	750	2800	3360	2800	1080	5	2040
0	0	590	2280	4635	2440	850	0	8160
0	0	510	2440	4635	2280	930	0	1360
35	240	640	0	8760	0	640	480	510

MMF functions on 8 variables

- It is known that any $F \in MMF$ on $n = 2k$ variables is concatenation of affine functions on k variables. This implies that there exists at least $\frac{(2^k-1)(2^{k-1}-1)}{3}$ many two dimensional subspaces such that with respect of each of them the second derivative of F is identically zero.
- For $k = 4$ this number is 35.
- The second-derivative spectrum of the constructed bent function does not contain the value 35.
- Thus F cannot be equivalent to a function in *MMF*.

MMF functions on 8 variables

- It is known that any $F \in MMF$ on $n = 2k$ variables is concatenation of affine functions on k variables. This implies that there exists at least $\frac{(2^k-1)(2^{k-1}-1)}{3}$ many two dimensional subspaces such that with respect of each of them the second derivative of F is identically zero.
- For $k = 4$ this number is 35.
- The second-derivative spectrum of the constructed bent function does not contain the value 35.
- Thus F cannot be equivalent to a function in *MMF*.

MMF functions on 8 variables

- It is known that any $F \in MMF$ on $n = 2k$ variables is concatenation of affine functions on k variables. This implies that there exists at least $\frac{(2^k-1)(2^{k-1}-1)}{3}$ many two dimensional subspaces such that with respect of each of them the second derivative of F is identically zero.
- For $k = 4$ this number is 35.
- The second-derivative spectrum of the constructed bent function does not contain the value 35.
- Thus F cannot be equivalent to a function in *MMF*.

MMF functions on 8 variables

- It is known that any $F \in MMF$ on $n = 2k$ variables is concatenation of affine functions on k variables. This implies that there exists at least $\frac{(2^k-1)(2^{k-1}-1)}{3}$ many two dimensional subspaces such that with respect of each of them the second derivative of F is identically zero.
- For $k = 4$ this number is 35.
- The second-derivative spectrum of the constructed bent function does not contain the value 35.
- Thus F cannot be equivalent to a function in *MMF*.

- Thus the bent function constructed above is neither equivalent to PS_{ap} nor to MMF.
- S. Gangopadhyay, A. Joshi, G. Leander and R. K. Sharma, A new construction of bent functions based on Z-bent functions. In: the proceedings of The Seventh International Workshop on Coding and Cryptography 2011. April 11–15, 2011, Paris, France, pp. 153–162.

- Thus the bent function constructed above is neither equivalent to PS_{ap} nor to MMF.
- S. Gangopadhyay, A. Joshi, G. Leander and R. K. Sharma, A new construction of bent functions based on Z-bent functions. In: the proceedings of The Seventh International Workshop on Coding and Cryptography 2011. April 11–15, 2011, Paris, France, pp. 153–162.

Thank you
Questions Please!