Orthogonal group, self-dual codes and Boolean functions

Presented by Lin SOK, Telecom ParisTech

October 26, 2011

Supervised by Patrick Solé, Telecom ParisTech

Outline

1. Self-dual codes and orthogonal group
2. Construction method
3. Classification of extremal codes
4. Self-dual bent functions and formally self-dual functions
5. Classification of self-dual bent functions

Outline

Outline

Outline

1. Self-dual codes and orthogonal group
2. Construction method
3. Classification of extremal codes
4. Self-dual bent functions and formally self-dual functions
5. Classification of self-dual bent functions

Outline

Definitions

- A binary linear $[n, k]$ code C: a k-dimensional subspace of $\mathbb{F}_2^n$
- $wt(x) := \#\{i : x_i \neq 0\}$, the (Hamming) weight of $x = (x_1, x_2, ..., x_n)$
- $d(C) := \min\{wt(x) : x \in C\}$, the minimum weight of C
- A $[n, k, d]$ code:a linear code of length n, dimension k and minimum weight d
- $C^\perp := \{x \in \mathbb{F}_2^n : \forall y \in C, x.y := \sum_{i=1}^n x_i y_i = 0\}$
- Self orthogonal if $C \subset C^\perp$ and self-dual if $C = C^\perp$
- A self-dual code C of Type II: $\forall x \in C, wt(x) \equiv 0 \pmod 4$
- A self-dual code C of Type I: not Type II

Definitions

- A binary linear $[n, k]$ code C: a k-dimensional subspace of $\mathbb{F}_2^n$
- $wt(x) := \#\{i : x_i \neq 0\}$, the (Hamming) weight of $x = (x_1, x_2, ..., x_n)$
- $d(C) := \min\{wt(x) : x \in C\}$, the minimum weight of C
- A $[n, k, d]$ code:a linear code of length n, dimension k and minimum weight d
- $C^\perp := \{x \in \mathbb{F}_2^n : \forall y \in C, x.y := \sum_{i=1}^n x_i y_i = 0\}$
- Self orthogonal if $C \subset C^\perp$ and self-dual if $C = C^\perp$
- A self-dual code C of Type II: $\forall x \in C, wt(x) \equiv 0 \pmod 4$
- A self-dual code C of Type I: not Type II

Definitions

- A binary linear $[n, k]$ code C: a k-dimensional subspace of $\mathbb{F}_2^n$
- $wt(x) := \#\{i : x_i \neq 0\}$, the (Hamming) weight of $x = (x_1, x_2, ..., x_n)$
- $d(C) := \min\{wt(x) : x \in C\}$, the minimum weight of C
- A $[n, k, d]$ code:a linear code of length n, dimension k and minimum weight d
- $C^\perp := \{x \in \mathbb{F}_2^n : \forall y \in C, x.y := \sum_{i=1}^n x_i y_i = 0\}$
- Self orthogonal if $C \subset C^\perp$ and self-dual if $C = C^\perp$
- A self-dual code C of Type II: $\forall x \in C, wt(x) \equiv 0 \pmod 4$
- A self-dual code C of Type I: not Type II

Definitions

- A binary linear $[n, k]$ code C: a k-dimensional subspace of $\mathbb{F}_2^n$
- $wt(x) := \#\{i : x_i \neq 0\}$, the (Hamming) weight of $x = (x_1, x_2, ..., x_n)$
- $d(C) := \min\{wt(x) : x \in C\}$, the minimum weight of C
- A $[n, k, d]$ code:a linear code of length n, dimension k and minimum weight d
- $C^\perp := \{x \in \mathbb{F}_2^n : \forall y \in C, x.y := \sum_{i=1}^n x_i y_i = 0\}$
- Self orthogonal if $C \subset C^\perp$ and self-dual if $C = C^\perp$
- A self-dual code C of Type II: $\forall x \in C, wt(x) \equiv 0 \pmod 4$
- A self-dual code C of Type I: not Type II

Definitions

- A binary linear $[n, k]$ code C: a k-dimensional subspace of $\mathbb{F}_2^n$
- $wt(x) := \#\{i : x_i \neq 0\}$, the (Hamming) weight of $x = (x_1, x_2, ..., x_n)$
- $d(C) := \min\{wt(x) : x \in C\}$, the minimum weight of C
- A $[n, k, d]$ code:a linear code of length n, dimension k and minimum weight d
- $C^\perp := \{x \in \mathbb{F}_2^n : \forall y \in C, x.y := \sum_{i=1}^n x_i y_i = 0\}$
- Self orthogonal if $C \subset C^\perp$ and self-dual if $C = C^\perp$
- A self-dual code C of Type II: $\forall x \in C, wt(x) \equiv 0 \pmod 4$
- A self-dual code C of Type I: not Type II

Definitions

- A binary linear $[n, k]$ code C: a k-dimensional subspace of $\mathbb{F}_2^n$
- $wt(x) := \#\{i : x_i \neq 0\}$, the (Hamming) weight of $x = (x_1, x_2, ..., x_n)$
- $d(C) := \min\{wt(x) : x \in C\}$, the minimum weight of C
- A $[n, k, d]$ code:a linear code of length n, dimension k and minimum weight d
- $C^{\perp} := \{x \in \mathbb{F}_2^n : \forall y \in C, x.y := \sum_{i=1}^{n} x_i y_i = 0\}$
- Self orthogonal if $C \subset C^{\perp}$ and self-dual if $C = C^{\perp}$
- A self-dual code C of Type II: $\forall x \in C, wt(x) \equiv 0 \pmod 4$
- A self-dual code C of Type I: not Type II

Definitions

- A binary linear $[n, k]$ code C: a k-dimensional subspace of $\mathbb{F}_2^n$
- $wt(x) := \#\{i : x_i \neq 0\}$, the (Hamming) weight of $x = (x_1, x_2, ..., x_n)$
- $d(C) := \min\{wt(x) : x \in C\}$, the minimum weight of C
- A $[n, k, d]$ code:a linear code of length n, dimension k and minimum weight d
- $C^\perp := \{x \in \mathbb{F}_2^n : \forall y \in C, x.y := \sum_{i=1}^n x_i y_i = 0\}$
- Self orthogonal if $C \subset C^\perp$ and self-dual if $C = C^\perp$
- A self-dual code C of Type II: $\forall x \in C, wt(x) \equiv 0 \pmod 4$
- A self-dual code C of Type I: not Type II

Definitions

- A binary linear $[n, k]$ code C: a k-dimensional subspace of $\mathbb{F}_2^n$
- $wt(x) := \#\{i : x_i \neq 0\}$, the (Hamming) weight of $x = (x_1, x_2, ..., x_n)$
- $d(C) := \min\{wt(x) : x \in C\}$, the minimum weight of C
- A $[n, k, d]$ code:a linear code of length n, dimension k and minimum weight d
- $C^\perp := \{x \in \mathbb{F}_2^n : \forall y \in C, x.y := \sum_{i=1}^n x_i y_i = 0\}$
- Self orthogonal if $C \subset C^\perp$ and self-dual if $C = C^\perp$
- A self-dual code C of Type II: $\forall x \in C, wt(x) \equiv 0 \pmod 4$
- A self-dual code C of Type I: not Type II

Facts

- If $C = C^{\perp}$ then
- • $n = 2k$.
- • $\forall x \in C, wt(x) \equiv 0 \ (mod 2)$.
- • $(1, 1, ..., 1) \in C$.
- If $(I_k|M)$ is a generator matrix for a self-dual code C then $MM^T = I_k$.
- $\mathcal{O}_n := \{M \in GL(n, \mathbb{F}_2) | MM^T = I_n\}$ is called the orthogonal group of $n \times n$ matrices over $\mathbb{F}_2$.

Facts

- If $C = C^{\perp}$ then
- • $n = 2k$.
- • $\forall x \in C, wt(x) \equiv 0 \ (mod 2)$.
- • $(1, 1, ..., 1) \in C$.
- If $(I_k|M)$ is a generator matrix for a self-dual code C then $MM^T = I_k$.
- $\mathcal{O}_n := \{M \in GL(n, \mathbb{F}_2) | MM^T = I_n\}$ is called the orthogonal group of $n \times n$ matrices over $\mathbb{F}_2$.

Facts

- If $C = C^{\perp}$ then
- • $n = 2k$.
- • $\forall x \in C, wt(x) \equiv 0 \ (mod 2)$.
- • $(1, 1, ..., 1) \in C$.
- If $(I_k|M)$ is a generator matrix for a self-dual code C then $MM^T = I_k$.
- $\mathcal{O}_n := \{M \in GL(n, \mathbb{F}_2) | MM^T = I_n\}$ is called the orthogonal group of $n \times n$ matrices over $\mathbb{F}_2$.

Facts

- If $C = C^{\perp}$ then
- • $n = 2k$.
- • $\forall x \in C, wt(x) \equiv 0 \ (mod 2)$.
- • $(1, 1, ..., 1) \in C$.
- If $(I_k|M)$ is a generator matrix for a self-dual code C then $MM^T = I_k$.
- $\mathcal{O}_n := \{M \in GL(n, \mathbb{F}_2) | MM^T = I_n\}$ is called the orthogonal group of $n \times n$ matrices over $\mathbb{F}_2$.

Facts

- If $C = C^{\perp}$ then
- • $n = 2k$.
- • $\forall x \in C, wt(x) \equiv 0 \ (mod 2)$.
- • $(1, 1, ..., 1) \in C$.
- If $(I_k|M)$ is a generator matrix for a self-dual code C then $MM^T = I_k$.
- $\mathcal{O}_n := \{M \in GL(n, \mathbb{F}_2) | MM^T = I_n\}$ is called the orthogonal group of $n \times n$ matrices over $\mathbb{F}_2$.

Facts

- If $C = C^{\perp}$ then
- • $n = 2k$.
- • $\forall x \in C, wt(x) \equiv 0 \ (mod 2)$.
- • $(1, 1, ..., 1) \in C$.
- If $(I_k|M)$ is a generator matrix for a self-dual code C then $MM^T = I_k$.
- $\mathcal{O}_n := \{M \in GL(n, \mathbb{F}_2) | MM^T = I_n\}$ is called the orthogonal group of $n \times n$ matrices over $\mathbb{F}_2$.

Generation theorem for orthogonal group

Theorem (Janusz)

Let $\mathcal{P}_n$ denote the group of all $n \times n$ permutation matrices, u a vector of even weight in $\mathbb{F}_2^n$ and $T_u : x \mapsto x + (x.u)u, \forall x \in \mathbb{F}_2^n$. Then the orthogonal group $\mathcal{O}_n$ are generated as follows
(1) for $1 \leq n \leq 3$, $\mathcal{O}_n = \mathcal{P}_n$,
(2) for $n \geq 4$, $\mathcal{O}_n =< \mathcal{P}_n, T_u >$, with $wt(u) = 4$.

Upper bound of minimum weight for self-dual code

Theorem (Rains and Sloane)

Let C be a binary self-dual code of length n then the minimum weight of C is upper bounded by

$$d(C) \leq \begin{cases} 4\left[\frac{n}{24}\right]+4, & \text{if } n \neq 22 \pmod{24}, \\ 4\left[\frac{n}{24}\right]+6, & \text{if } n = 22 \pmod{24}. \end{cases}$$

Numerical result for some extremal codes

- Definition
  A self-dual C is called extremal if $d(C)$ attains one of the bounds above.

- Theorem
  There are at least 288 *extremal codes of length* 56 *and at least* 71 *extremal codes of length* 74.

Numerical result for some extremal codes

- Definition
  A self-dual C is called extremal if $d(C)$ attains one of the bounds above.

- Theorem
  There are at least 288 *extremal codes of length* 56 *and at least* 71 *extremal codes of length* 74.

Subtraction procedure (11)

- $[n+2, n/2+1, d+2] \rightarrow [n, n/2, \geq d]$
- •

$$G_{n+2} = \begin{bmatrix} 0 & 1 & \\ a_1 & a_1 & \\ \vdots & \vdots & G'_n \\ a_{\frac{n}{2}} & a_{\frac{n}{2}} & \end{bmatrix}$$

Subtraction procedure (11)

- $[n+2, n/2+1, d+2] \to [n, n/2, \geq d]$
- •

$$G_{n+2} = \left[\begin{array}{ccc} 0 & 1 & \\ a_1 & a_1 & \\ \vdots & \vdots & G'_n \\ a_{\frac{n}{2}} & a_{\frac{n}{2}} & \end{array}\right]$$

Recursive construction (Gaborit and Melchor)

- $[n, n/2, \geq d] \rightarrow [n+2, n/2+1, d+2]$
- •
$$G_n = \begin{bmatrix} G_d \\ G_E \end{bmatrix}$$
- •
$$G'_{n+2} = \begin{bmatrix} 1 & 1 & \\ \vdots & \vdots & G_d \\ 1 & 1 & \\ a_1 & a_1 & \\ \vdots & \vdots & G_E \\ a_{\frac{n}{2}-k} & a_{\frac{n}{2}-k} & \end{bmatrix}$$

Recursive construction (Gaborit and Melchor)

- $[n, n/2, \geq d] \rightarrow [n+2, n/2+1, d+2]$
- •
$$G_n = \begin{bmatrix} G_d \\ G_E \end{bmatrix}$$
- •
$$G'_{n+2} = \begin{bmatrix} 1 & 1 & \\ \vdots & \vdots & G_d \\ 1 & 1 & \\ a_1 & a_1 & \\ \vdots & \vdots & G_E \\ a_{\frac{n}{2}-k} & a_{\frac{n}{2}-k} & \end{bmatrix}$$

Recursive construction (Gaborit and Melchor)

- $[n, n/2, \geq d] \to [n+2, n/2+1, d+2]$
- •
$$G_n = \begin{bmatrix} G_d \\ G_E \end{bmatrix}$$
- •
$$G'_{n+2} = \begin{bmatrix} 1 & 1 & \\ \vdots & \vdots & G_d \\ 1 & 1 & \\ a_1 & a_1 & \\ \vdots & \vdots & G_E \\ a_{\frac{n}{2}-k} & a_{\frac{n}{2}-k} & \end{bmatrix}$$

Dimensions of subcodes of 58671 $[36, 18, 6]$ codes

dim k	num	dim k	num	dim k	num
2	148	8	4615	14	8170
3	5	9	911	15	5311
4	666	10	7165	16	6290
5	45	11	2299	17	4492
6	2165	12	8411	18	3615
7	263	13	4100		

- In terms of equivalence test, the recursive construction is very fast since most of the subcodes are of large dimension k.

Dimensions of subcodes of 58671 $[36, 18, 6]$ codes

dim k	num	dim k	num	dim k	num
2	148	8	4615	14	8170
3	5	9	911	15	5311
4	666	10	7165	16	6290
5	45	11	2299	17	4492
6	2165	12	8411	18	3615
7	263	13	4100		

- In terms of equivalence test, the recursive construction is very fast since most of the subcodes are of large dimension k.

Classificaion of extremal [38,19,8] self-dual codes

Theorem

There are exactly 2744 inequivalent self-dual [38,19,8] codes.

Boolean functions

- Boolean function: $f : \mathbb{F}_2^n \to \mathbb{F}_2$
- Truth table: $f := (f_0, f_1, \cdots, f_{2^n-1})$, $f_a := f(a)$ with $a := \sum_{i=1}^n a_i 2^i := a_1 a_2 \cdots a_n \in \mathbb{F}_2^n$
- Sign function: $F := (-1)^f := ((-1)^{f_0}, (-1)^{f_1}, \cdots, (-1)^{f_{2^n-1}}) \in \{-1, 1\}^{2^n}$
- Support code of f: $C_f := \{u \in \mathbb{F}_2^n : f(u) = 1\}$
- Walsh-Hadamard transform (WHT) of f: $\hat{F}(u) := \sum_{v \in \mathbb{F}_2^n} (-1)^{f(v)+u.v}$
- Matrix form of WHT: $\hat{F} = FH_n$, with $H_1 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $H_n := \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}$

Boolean functions

- Boolean function: $f : \mathbb{F}_2^n \to \mathbb{F}_2$
- Truth table: $f := (f_0, f_1, \cdots, f_{2^n-1})$, $f_a := f(a)$ with $a := \sum_{i=1}^n a_i 2^i := a_1 a_2 \cdots a_n \in \mathbb{F}_2^n$
- Sign function: $F := (-1)^f := ((-1)^{f_0}, (-1)^{f_1}, \cdots, (-1)^{f_{2^n-1}}) \in \{-1, 1\}^{2^n}$
- Support code of f: $C_f := \{u \in \mathbb{F}_2^n : f(u) = 1\}$
- Walsh-Hadamard transform (WHT) of f: $\hat{F}(u) := \sum_{v \in \mathbb{F}_2^n} (-1)^{f(v)+u.v}$
- Matrix form of WHT: $\hat{F} = FH_n$, with $H_1 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $H_n := \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}$

Boolean functions

- Boolean function: $f : \mathbb{F}_2^n \to \mathbb{F}_2$
- Truth table: $f := (f_0, f_1, \cdots, f_{2^n-1})$, $f_a := f(a)$ with $a := \sum_{i=1}^n a_i 2^i := a_1 a_2 \cdots a_n \in \mathbb{F}_2^n$
- Sign function: $F := (-1)^f := ((-1)^{f_0}, (-1)^{f_1}, \cdots, (-1)^{f_{2^n-1}}) \in \{-1, 1\}^{2^n}$
- Support code of f: $C_f := \{u \in \mathbb{F}_2^n : f(u) = 1\}$
- Walsh-Hadamard transform (WHT) of f: $\hat{F}(u) := \sum_{v \in \mathbb{F}_2^n} (-1)^{f(v)+u.v}$
- Matrix form of WHT: $\hat{F} = FH_n$, with $H_1 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $H_n := \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}$

Boolean functions

- Boolean function: $f : \mathbb{F}_2^n \to \mathbb{F}_2$
- Truth table: $f := (f_0, f_1, \cdots, f_{2^n-1})$, $f_a := f(a)$ with $a := \sum_{i=1}^{n} a_i 2^i := a_1 a_2 \cdots a_n \in \mathbb{F}_2^n$
- Sign function: $F := (-1)^f := ((-1)^{f_0}, (-1)^{f_1}, \cdots, (-1)^{f_{2^n-1}}) \in \{-1, 1\}^{2^n}$
- Support code of f: $C_f := \{u \in \mathbb{F}_2^n : f(u) = 1\}$
- Walsh-Hadamard transform (WHT) of f: $\hat{F}(u) := \sum_{v \in \mathbb{F}_2^n} (-1)^{f(v)+u.v}$
- Matrix form of WHT: $\hat{F} = FH_n$, with $H_1 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $H_n := \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}$

Boolean functions

- Boolean function: $f : \mathbb{F}_2^n \to \mathbb{F}_2$
- Truth table: $f := (f_0, f_1, \cdots, f_{2^n-1})$, $f_a := f(a)$ with $a := \sum_{i=1}^{n} a_i 2^i := a_1 a_2 \cdots a_n \in \mathbb{F}_2^n$
- Sign function: $F := (-1)^f := ((-1)^{f_0}, (-1)^{f_1}, \cdots, (-1)^{f_{2^n-1}}) \in \{-1, 1\}^{2^n}$
- Support code of f: $C_f := \{u \in \mathbb{F}_2^n : f(u) = 1\}$
- Walsh-Hadamard transform (WHT) of f: $\hat{F}(u) := \sum_{v \in \mathbb{F}_2^n} (-1)^{f(v)+u.v}$
- Matrix form of WHT: $\hat{F} = FH_n$, with $H_1 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $H_n := \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}$

Self-dual bent functions

- f is called bent if $\hat{F}(u) = \pm 2^{n/2}, \forall u \in \mathbb{F}_2^n$.
- If f is bent then there exists a function $\tilde{f}$ with its sign function $\tilde{F}$ such that $FH_n = 2^{\frac{n}{2}} \tilde{F}$.
- f is called self-dual if $f = \tilde{f}$.
- f is self-dual iff $F = 2^{-\frac{n}{2}} FH_n$.

Self-dual bent functions

- f is called bent if $\hat{F}(u) = \pm 2^{n/2}, \forall u \in \mathbb{F}_2^n$.
- If f is bent then there exists a function $\tilde{f}$ with its sign function $\tilde{F}$ such that $FH_n = 2^{\frac{n}{2}} \tilde{F}$.
- f is called self-dual if $f = \tilde{f}$.
- f is self-dual iff $F = 2^{-\frac{n}{2}} FH_n$.

Self-dual bent functions

- f is called bent if $\hat{F}(u) = \pm 2^{n/2}, \forall u \in \mathbb{F}_2^n$.
- If f is bent then there exists a function $\tilde{f}$ with its sign function $\tilde{F}$ such that $FH_n = 2^{\frac{n}{2}}\tilde{F}$.
- f is called self-dual if $f = \tilde{f}$.
- f is self-dual iff $F = 2^{-\frac{n}{2}}FH_n$.

Self-dual bent functions

- f is called bent if $\hat{F}(u) = \pm 2^{n/2}, \forall u \in \mathbb{F}_2^n$.
- If f is bent then there exists a function $\tilde{f}$ with its sign function $\tilde{F}$ such that $FH_n = 2^{\frac{n}{2}}\tilde{F}$.
- f is called self-dual if $f = \tilde{f}$.
- f is self-dual iff $F = 2^{-\frac{n}{2}} FH_n$.

Some known results

- Theorem (Carlet, Danielsen, Parker and Solé)
  If f self-dual bent function, $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2, b \in \mathbb{F}_2^n$, $wt(b)$ even, then $g(x) = f(L(x+b)) + b \cdot x + c$ is also self-dual bent. In this case we say that g and f are equivalent.
- Theorem (Carlet, Danielsen, Parker and Solé)
  There are 1, 2 and 8 equivalence classes of self-dual bent functions in 2,4 and 6 variables respectively.

Some known results

- Theorem (Carlet, Danielsen, Parker and Solé)
  If f self-dual bent function, $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2, b \in \mathbb{F}_2^n$, $wt(b)$ even, then $g(x) = f(L(x+b)) + b \cdot x + c$ is also self-dual bent. In this case we say that g and f are equivalent.
- Theorem (Carlet, Danielsen, Parker and Solé)
  There are 1, 2 and 8 equivalence classes of self-dual bent functions in 2,4 and 6 variables respectively.

Formally self-dual functions

- Weight enumerator of a code C of length n: $W_C(x,y) := \sum_{i=0}^{n} A_i(C)x^i y^{n-i}$, $A_i(C)$: number of weight-i codewords in C
- Formally self-dual code w.r.t W_C: $W_C(x,y) = W_C(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}})$
- Near weight enumerator of a code C: $W_C^+(x,y) := 2^{\frac{n}{2}-1}x^n + W_C(x,y)$
- f, formally self-dual function w.r.t its near weight enumerator : C_f, formally self-dual code w.r.t $W_{C_f}^+$

Formally self-dual functions

- Weight enumerator of a code C of length n: $W_C(x,y) := \sum_{i=0}^{n} A_i(C)x^i y^{n-i}$, $A_i(C)$: number of weight-i codewords in C
- Formally self-dual code w.r.t W_C: $W_C(x,y) = W_C(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}})$
- Near weight enumerator of a code C: $W_C^+(x,y) := 2^{\frac{n}{2}-1}x^n + W_C(x,y)$
- f, formally self-dual function w.r.t its near weight enumerator : C_f, formally self-dual code w.r.t $W_{C_f}^+$

Formally self-dual functions

- Weight enumerator of a code C of length n: $W_C(x,y) := \sum_{i=0}^{n} A_i(C)x^i y^{n-i}$, $A_i(C)$: number of weight-i codewords in C
- Formally self-dual code w.r.t W_C: $W_C(x,y) = W_C(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}})$
- Near weight enumerator of a code C: $W_C^+(x,y) := 2^{\frac{n}{2}-1}x^n + W_C(x,y)$
- f, formally self-dual function w.r.t its near weight enumerator : C_f, formally self-dual code w.r.t $W_{C_f}^+$

Formally self-dual functions

- Weight enumerator of a code C of length n: $W_C(x,y) := \sum_{i=0}^{n} A_i(C)x^i y^{n-i}$, $A_i(C)$: number of weight-i codewords in C
- Formally self-dual code w.r.t W_C: $W_C(x,y) = W_C(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}})$
- Near weight enumerator of a code C: $W_C^+(x,y) := 2^{\frac{n}{2}-1}x^n + W_C(x,y)$
- f, formally self-dual function w.r.t its near weight enumerator : C_f, formally self-dual code w.r.t $W_{C_f}^+$

Propositions

- Proposition (Hyun, Lee and Lee)

  Let f be a formally self-dual function in n variables with respect its near weight enumerator. Then

$$W_{C_f}(x,y) = -2^{\frac{n}{2}-1}x^n + \sum_{j=0}^{\frac{n}{2}} a_j(x^2+y^2)(xy-y^2)^j, \qquad (1)$$

  where a_j's are integers.

- Proposition (Hyun, Lee and Lee)

  Every self-dual bent function is formally self-dual function with respect to its near weight enumerator.

Propositions

- Proposition (Hyun, Lee and Lee)

  Let f be a formally self-dual function in n variables with respect its near weight enumerator. Then

  $$W_{C_f}(x,y) = -2^{\frac{n}{2}-1}x^n + \sum_{j=0}^{\frac{n}{2}} a_j(x^2+y^2)(xy-y^2)^j, \qquad (1)$$

  where a_j's are integers.

- Proposition (Hyun, Lee and Lee)

  Every self-dual bent function is formally self-dual function with respect to its near weight enumerator.

Weight distributions of support

Table: Weight distributions of support code for $n = 2$

i	0	1	2
A_i^1	0	0	1
A_i^2	1	1	1
A_i^3	0	1	0
A_i^4	1	2	0

- With weight distribution $A_i^1 = [0, 0, 1]$, the formally self-dual function is of weight $1 = 0 + 0 + 1$ and it corresponds to a codeword $(f = (f_0, f_1, f_2, f_3) = (0, 0, 0, 1))$ of weight 1 in the Reed-Muller code $RM(2, 2)$.
- We have additional information on weight of formally self-dual functions (self-dual bent functions) that are codewords of ReedMuller code.

Weight distributions of support

Table: Weight distributions of support code for $n = 2$

i	0	1	2
A_i^1	0	0	1
A_i^2	1	1	1
A_i^3	0	1	0
A_i^4	1	2	0

- With weight distribution $A_i^1 = [0, 0, 1]$, the formally self-dual function is of weight $1 = 0 + 0 + 1$ and it corresponds to a codeword ($f = (f_0, f_1, f_2, f_3) = (0, 0, 0, 1)$) of weight 1 in the Reed-Muller code $RM(2, 2)$.
- We have additional information on weight of formally self-dual functions (self-dual bent functions) that are codewords of ReedMuller code.

Weight distributions of support

Table: Weight distributions of support code for $n = 2$

i	0	1	2
A_i^1	0	0	1
A_i^2	1	1	1
A_i^3	0	1	0
A_i^4	1	2	0

- With weight distribution $A_i^1 = [0, 0, 1]$, the formally self-dual function is of weight $1 = 0 + 0 + 1$ and it corresponds to a codeword $(f = (f_0, f_1, f_2, f_3) = (0, 0, 0, 1))$ of weight 1 in the Reed-Muller code $RM(2, 2)$.
- We have additional information on weight of formally self-dual functions (self-dual bent functions) that are codewords of ReedMuller code.

Table: Weight distributions of support code for $n = 4$

i	0	1	2	3	4
A_i^1	0	0	3	2	1
A_i^2	0	0	2	4	0
A_i^3	0	1	3	1	1
A_i^4	0	1	2	3	0
A_i^5	0	2	2	2	0
A_i^6	0	2	3	0	1
A_i^7	0	3	2	1	0
A_i^8	0	4	2	0	0
A_i^9	1	0	4	4	1
A_i^{10}	1	1	4	3	1
A_i^{11}	1	2	4	2	1
A_i^{12}	1	2	3	4	0
A_i^{13}	1	3	3	3	0
A_i^{14}	1	3	4	1	1
A_i^{15}	1	4	3	2	0
A_i^{16}	1	4	4	0	1

Deducing self-dual bent functions

To deduce the self-dual bent functions in n variables of degree r

- Calculate the weight distributions of support code and then the weights $d_j (= |C_f|)$ of the corresponding formally self-dual functions.
- for each codeword f of weights d_j in $RM(r, n)$, if $F = 2^{-\frac{n}{2}} F H_n$ then f is self-dual bent.

Deducing self-dual bent functions

To deduce the self-dual bent functions in n variables of degree r

- Calculate the weight distributions of support code and then the weights $d_j (= |C_f|)$ of the corresponding formally self-dual functions.
- for each codeword f of weights d_j in $RM(r, n)$, if $F = 2^{-\frac{n}{2}} F H_n$ then f is self-dual bent.

Thank you!