Dual transform and projective self-dual codes

Iliya Bouyukliev
Bulgarian Academy of Sciences

Joint work with Stefka Bouyuklieva
St. Cyril and St. Methodius University of Veliko Tarnovo, BULGARIA

February 2023, Marseille

Outline

C - a linear $[n, k, d]$ code over $GF(q)$

- $\mathbb{F}_q$ (or $GF(q)$) - a finite field with q elements;
- $\mathbb{F}_q^n$ - n-dimensional vector space over $\mathbb{F}_q$;
- Weight of a vector $x \in \mathbb{F}_q^n$: $\mathrm{wt}(x) = |\{i | x_i \neq 0\}|$;
- Linear code of length n and dimension k - k-dimensional subspace of $\mathbb{F}_q^n$;
- Minimum weight (or minimum distance) of a linear code C:

$$d(C) = \min\{\mathrm{wt}(x) | x \in C,\ x \neq \mathbf{0}\}$$

- C - linear $[n, k, d]_q$ code.

C - linear $[n, k, d]_q$ code

A generator matrix of C

$$G = \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix} = (b_1\ b_2\ \cdots\ b_n)$$

$$C = \langle G \rangle = \{\alpha_1 a_1 + \cdots + \alpha_k a_k, (\alpha_1, \ldots, \alpha_k) \in \mathbb{F}_q^k\}$$

Weight spectrum of C: $(A_0, A_1, \ldots, A_n) \in \mathbb{Z}^{n+1}$

A_i - the number of codewords of weight i

Weight function of C: $W_C(y) = A_0 + A_1 y + A_2 y^2 + \cdots + A_n y^n$

C - a linear $[n, k, d]$ code over $GF(q)$

Let G be a generator matrix of C.

- The columns of G represent points of the projective geometry $PG(k-1, q)$.
- We can consider the code as a multiset $\mathcal{C}$ of n points in $PG(k-1, q)$. Each hyperplane of $PG(k-1, q)$ meets $\mathcal{C}$ in at most $n-d$ points.
- Two codes are equivalent if and only if the corresponding multisets of points are projectively equivalent.

Dual Transform

There are different definitions for the (projective) dual transform. Usually the transform is defined constructively using different structures:

- in terms of projective geometry - Delsarte (1972), Ray Hill (1978), Brouwer and van Eupen (1997), Dodunekov and Simonis (1998), Nogin (1998);
- using matrices - Iliya Bouyukliev (2009).

We use characteristic vectors!

Dual transform - motivation

Projective dual transform is important for

- construction of linear codes;
- classification of linear codes;
- proofs for nonexistence of linear codes with given parameters;
- construction and classification of infinite families of codes;
- relations between linear codes, projective geometries, incidence structures, Boolean functions.

Motivating references:

- S. Dodunekov and J. Simonis, Codes and projective multisets, *Electron. J. Combin.* 1998.
- I. Bouyukliev, Classification of Griesmer Codes and Dual Transform, *Discrete Mathematics*, 2009.
- Bouyukliev, Bouyuklieva, Pashinska-Gadzheva, On Some Families of Codes Related to the Even Linear Codes Meeting the Grey-Rankin Bound, *Mathematics*, 2022.

Dual transform (Brouwer and Van Eupen)

Let C be a linear $[n, k, d]_q$ code with a generator matrix G

$W = \{w_1, w_2, \ldots, w_s\}$ - the set of all nonzero weights in C

Let $\alpha, \beta \in \mathbb{Q}$ such that $\alpha w_i + \beta$ are nonnegative integers for all i

Consider a maximal set $\mathbb{P}$ of nonzero vectors $v \in \mathbb{F}_q^k$ for which the corresponding points in $PG(k-1, q)$ are different.

Definition: The dual code $D_{\alpha,\beta}(C)$ of C is the code generated by the matrix $D_{\alpha,\beta}(G)$ whose columns are all vectors $v \in \mathbb{P}$ taken $\alpha wt(vG) + \beta$ times.

Dual transform (Brouwer and Van Eupen)
$[11, 3, 8]_5$ code

$$G = \begin{pmatrix} 11111110100 \\ 12233444010 \\ 43030414101 \end{pmatrix}, \quad W = \{8, 9, 10, 11\}$$

$$\alpha = 1, \quad \beta = -8$$

$$\begin{aligned}
(001)G &= (43030414101) \text{ - weight } 8, && \Rightarrow 8\alpha + \beta = 0, \\
(010)G &= (12233444010) \text{ - weight } 9, && \Rightarrow 9\alpha + \beta = 1, \\
(011)G &= (00213303111) \text{ - weight } 8, && \Rightarrow 8\alpha + \beta = 0, \\
(012)G &= (43243212212) \text{ - weight } 11, && \Rightarrow 11\alpha + \beta = 3, \\
&\vdots && \vdots
\end{aligned}$$

$$\Rightarrow D_{1,-8}(G) = \begin{pmatrix} 00000001111111111111111111 \\ 11111110011111111122334444444 \\ 02223332211123332213011233 4 \end{pmatrix}$$

$D_{\alpha,\beta}(C)$ - a linear $[27, 3, 20]_5$ code

Dual transform (Brouwer and Van Eupen)
$[6, 4, 2]_2$ code

$$G = \begin{pmatrix} 000011 \\ 001100 \\ 010001 \\ 100100 \end{pmatrix}, \quad W = \{2, 4\}, \quad \alpha = 1/2, \quad \beta = -1$$

$$\begin{aligned}
(0001)G &= (100100) \text{ - weight 2}, && \Rightarrow 2\alpha + \beta = 0, \\
(0010)G &= (010001) \text{ - weight 2}, && \Rightarrow 2\alpha + \beta = 0, \\
(0011)G &= (110101) \text{ - weight 4}, && \Rightarrow 4\alpha + \beta = 1, \\
(0100)G &= (001100) \text{ - weight 2}, && \Rightarrow 2\alpha + \beta = 0, \\
&\vdots && \vdots
\end{aligned}$$

$$\Rightarrow D_{1/2,-1}(G) = \begin{pmatrix} 000111111 \\ 011001111 \\ 111010011 \\ 101110101 \end{pmatrix}, \quad D_{1/2,-1}(C) - [9, 4, 6]_2 \text{ code}$$

The simplex code $S(q,k)$

- The columns in a generator matrix of $S(q,k)$ are all points in the projective geometry $PG(k-1,q)$.
- $S(q,k)$ - a linear $[\theta(q,k)=\frac{q^k-1}{q-1},k,q^{k-1}]_q$ code
- Consider the generator matrix G_k of $S(q,k)$, following the recurrence relation

$$G_1=(1),\quad G_2=\begin{pmatrix}0&1&1&\dots&1\\1&0&1&\dots&\alpha_{q-2}\end{pmatrix},$$

$$G_{k+1}=\begin{pmatrix}0&1&1&\dots&1\\G_k&0&G_k&\dots&\alpha_{q-2}G_k\end{pmatrix}\text{ for } k\geq 1,$$

where $\mathbb{F}_q=\{0,1,\dots,\alpha_{q-2}\}$.

The simplex code $S(q,k)$

Consider the following matrices:

- $M_k = G_k^T \cdot G_k$ - a symmetric q-ary $\theta(q,k) \times \theta(q,k)$ matrix, whose rows are nonproportional codewords in the simplex code $S_{q,k}$.
- $\mathcal{N}(M_k)$ - the binary matrix obtained from M_k by replacing all nonzero elements by 1. We consider $\mathcal{N}(M_k)$ as an integer matrix.
- $$\mathcal{N}(M_k)^2 = q^{k-2} \begin{pmatrix} q & q-1 & \dots & q-1 \\ q-1 & q & \dots & q-1 \\ \vdots & \vdots & \ddots & \vdots \\ q-1 & q-1 & \dots & q \end{pmatrix}.$$

Characteristic vector - definition

Let C be a k-dimensional linear code over $\mathbb{F}_q$ and G be an $m \times n$ matrix which generates the code.

The *characteristic vector* of the $[n, k; q]$-code C with respect to the matrix G is

$$\chi(C, G) = (\chi_1, \chi_2, \ldots, \chi_{\theta(q,m)}) \in \mathbb{Z}^{\theta(q,k)}$$

where χ_i is the number of the columns of G that are equal or proportional (with nonzero coefficients) to the i-th column of the matrix G_m.

The generator matrix, corresponding to the characteristic vector χ, is denoted by G_χ.

Characteristic vector - $[11, 3, 8]_5$ code

$$G = \begin{pmatrix} 11111110100 \\ 12233444010 \\ 43030414101 \end{pmatrix}$$

$$G_4 = \begin{pmatrix} 00000011111111111111111111111111 \\ 01111100111111022222033333044444 \\ 10123401012342024133031424043 21 \end{pmatrix}$$

$$\chi(C, G) = (11100001000010100010110000010 01) \in \mathbb{Z}^{31}$$

Characteristic vector - $[6, 4, 2]_2$ code

$$G = \begin{pmatrix} 000011 \\ 001100 \\ 010001 \\ 100100 \end{pmatrix}$$

$$G_3 = \begin{pmatrix} 000000011111111 \\ 000111100001111 \\ 011001100110011 \\ 101010101010101 \end{pmatrix}$$

$$\chi(C, G) = (110110010100000) \in \mathbb{Z}^{15}$$

Characteristic vector - properties

Let C be a k-dimensional linear code over $\mathbb{F}_q$ and G be an $m \times n$ matrix which generates the code.

- $\sum_{i=1}^{\theta(q,k)} \chi_i = n$
- If $\chi \cdot \mathcal{N}(M_m) = (\omega_1, \ldots, \omega_{\theta(q,m)}) \in \mathbb{Z}^{\theta(q,m)}$, then $\omega_i = \mathrm{wt}(v_i)$ where v_i is the i-th row of the matrix $G_m^T \cdot G$.
- The coordinates of $\chi \cdot \mathcal{N}(M_k)$ gives the weights of a maximal set of nonproportional codewords in C (k is the dimension of C).

Dual transform

Definition: Let α and β be rational numbers such that $\alpha w_i + \beta \in \mathbb{Z}$ for any nonzero weight w of a codeword in C. The *projective dual code* $D_{\alpha,\beta,m}(C)$ of C is the linear code with characteristic vector $\chi_{\alpha,\beta,m} = \alpha\chi \cdot \mathcal{N}(M_m) + \beta.\mathbf{1}$, where $\mathbf{1}$ is the all-ones vector of the corresponding length.

Example: $\chi(C, G) = (11100010000010100010110000010 01)$

$$\Rightarrow \chi_{1,-8,3} = \chi \cdot \mathcal{N}(M_3) - (88 \ldots 8)$$
$$= (01033000031302020000011000112 12)$$

Parameters of the projective dual code

- Length $n_{\alpha,\beta,m} = \alpha \sum_{i=1}^{\theta(q,m)} \omega_i + \beta\theta(q,m)$

$$= \alpha \sum_{i=1}^{\theta(q,m)} wt(v_i) + \beta\theta(q,m) = \alpha n q^{m-1} + \beta\theta(q,m)$$

- Weights - the coordinates of

$$\chi_{\alpha,\beta,m} \cdot \mathcal{N}(M_m) = \alpha\chi \cdot \mathcal{N}(M_m)^2 + (\beta.\mathbf{1}) \cdot \mathcal{N}(M_m)$$

$$= \alpha q^{m-2}(\chi_1 + (q-1)n, \ldots, \chi_\theta + (q-1)n) + \beta q^{m-1}\mathbf{1}$$

$$= q^{m-2}(\alpha\chi_1 + \alpha(q-1)n + \beta q, \ldots, \alpha\chi_\theta + \alpha(q-1)n + \beta q).$$

Parameters of the projective dual code

The example: $[11, 3, 8]_5$ code

- Length $n_{1,-8,3} = 11.5^2 - 8.31 = 27$.
- Weights - the coordinates of $\chi_{1,-8,3} \cdot \mathcal{N}(M_m)$
  $= (25, 25, 25, 20, 20, 20, 20, 25, 20, 20, 20, 20, 25, 20, 25,$
  $20, 20, 20, 25, 20, 25, 25, 20, 20, 20, 20, 20, 25, 20, 20, 25)$
  Hence $D_{1,-8,3}(C)$ is a two-weight code with nonzero weights 20 and 25.

Lemma: If C is a projective linear code then its dual code has at most two nonzero weights.

Invertibility

Lemma: If C is a linear q-ary code, then C is the projective dual code to $D_{\alpha,\beta,m}(C)$ for $\lambda = \frac{1}{\alpha q^{m-2}}$ and $\mu = -\frac{\alpha(q-1)n+\beta q}{\alpha}$.

Proof:

$$\lambda\chi_{\alpha,\beta,m} \cdot \mathcal{N}(M_m) + \mu.\mathbf{1} = \lambda\alpha\chi \cdot \mathcal{N}(M_m)^2 + \lambda\beta \cdot \mathbf{1} \cdot \mathcal{N}(M_m) + \mu.\mathbf{1}$$

$$= \lambda\alpha(q^{m-2}\chi + q^{m-2}(q-1)n.\mathbf{1}) + \lambda\beta q^{m-1} \cdot \mathbf{1} + \mu.\mathbf{1}$$

$$= \lambda\alpha q^{m-2}\chi + (\lambda\alpha(q-1)q^{m-2}n + \lambda\beta q^{m-1} + \mu).\mathbf{1}$$

If χ and $\mathbf{1}$ are not proportional, then

$$\lambda\alpha q^{m-2}\chi + (\lambda\alpha(q-1)q^{m-2}n + \lambda\beta q^{m-1} + \mu).\mathbf{1} = \chi$$

$$\iff \lambda = \frac{1}{\alpha q^{m-2}}, \quad \mu = -\frac{\alpha(q-1)n+\beta q}{\alpha}.$$

Hence χ is the characteristic vector of $D_{\lambda,\mu,m}(D_{\alpha,\beta,m}(C))$ and therefore this code is equivalent to C.

Projective self-dual codes

Definition: The linear code C is projective self-dual if it is equivalent to its projective dual code for some α, β, and $m = k$.

Lemma

If C is a linear q-ary code, then C is the projective dual code to $D_{\alpha,\beta,m}(C)$ for $\lambda = \frac{1}{\alpha q^{m-2}}$ and $\mu = -\frac{\alpha(q-1)n+\beta q}{\alpha}$.

Lemma

Let C be q-ary $[n, k, d]$ projective self-dual code. If C is not a replicated simplex code, then $\alpha = \pm q^{1-\frac{k}{2}}, \quad \beta = -\frac{q-1}{1+q^{k-1}\alpha} n$.

Projective self-dual codes - $[6, 4, 2]_2$ code

$$G = \begin{pmatrix} 000011 \\ 001100 \\ 110101 \\ 100100 \end{pmatrix}, \quad W = \{2, 4\} \quad \alpha = -1/2, \quad \beta = 2$$

$$\chi(C, G) = (011100110100000) \in \mathbb{Z}^{15}$$

$$\begin{aligned} \Rightarrow \chi_{-1/2,2,4} &= (-1/2)\chi \cdot \mathcal{N}(M_4) + (22 \ldots 2) \\ &= (101110010010000) \end{aligned}$$

Is there another characteristic vector χ' of the same code (or an equivalent code) such that ${\chi'}_{-1/2,2,4} = \chi'$?

Projective self-dual codes and incidence structures

Definition

An incidence structure $S = (P, B, I)$ is **self-dual** if it is isomorphic to its dual (B, P, I^T): that is, if there are bijections $f : P \to B$ and $g : B \to P$ such that $(g(b), f(p)) \in I$ if and only if $(p, b) \in I$. It is **self-polar** if we can choose $g = f^{-1}$.

Equivalently, using the incidence matrix N:

- $S = (P, B, I)$ is **self-dual** if there exist permutation matrices P_1 and P_2 such that $P_1 N = N^T P_2$;
- $S = (P, B, I)$ is **self-polar** if there exist a permutation matrix P such that $PN = N^T P^T$.

A.E. Brouwer, Peter J. Cameron, W.H. Haemers, D.A. Preece, *Self-dual, not self-polar*, Discrete Mathematics, 2006.

Projective self-dual codes and incidence structures

Let C be a linear code with a generator matrix G and $G_{\chi_{\alpha,\beta,m}}$ is the corresponding generator matrix of the dual code $D_{\alpha,\beta,m}(C)$. We consider the matrix $N = G^T_{\chi_{\alpha,\beta,m}} G$ as the incidence matrix of an incidence structure. Then we have the following definitions:

- C is **projective self-dual** if there exist permutation matrices P_1 and P_2 such that $P_1 N = N^T P_2$;
- C is **self-polar** if there exist a permutation matrix P such that $PN = N^T P^T$ (N is equivalent to a symmetric matrix).

Projective self-dual codes - $[6, 4, 2]_2$ code

$$G = \begin{pmatrix} 000011 \\ 001100 \\ 010001 \\ 100100 \end{pmatrix}, \quad W = \{2, 4\} \quad \alpha = -1/2, \quad \beta = 2$$

$$\chi(C, G) = (110110010100000) \in \mathbb{Z}^{15}$$

$$\begin{aligned} \Rightarrow \chi_{-1/2,2,4} &= (-1/2)\chi \cdot \mathcal{N}(M_4) + (22 \ldots 2) \\ &= (110110010100000) \end{aligned}$$

Projective self-dual codes - $[6, 4, 2]_2$ code

$$G = \begin{pmatrix} 010001 \\ 001100 \\ 101000 \\ 000011 \end{pmatrix}, \quad W = \{2, 4\} \quad \alpha = -1/2, \quad \beta = 2$$

$$\chi(C, G) = (1101100101000000) = \chi_{-1/2,2,4}$$

$$G^T G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Projective self-dual codes - $[6, 4, 2]_2$ code

$$\left(\begin{array}{cccccccccccccccc}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
\hline
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
\hline
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
\hline
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
\hline
0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
\hline
1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0
\end{array}\right)
\cdot
\begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}
=
\begin{pmatrix} 2 \\ 2 \\ 4 \\ 2 \\ 2 \\ 4 \\ 4 \\ 2 \\ 4 \\ 2 \\ 4 \\ 4 \\ 4 \\ 4 \end{pmatrix}$$

Projective self-dual codes - $[6, 4, 2]_2$ code

$$-\frac{1}{2}\begin{pmatrix} 2 \\ 2 \\ 4 \\ 2 \\ 2 \\ 4 \\ 4 \\ 2 \\ 4 \\ 2 \\ 4 \\ 4 \\ 4 \\ 4 \end{pmatrix} + 2\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Projective self-dual codes - $[6, 4, 2]_2$ code

$$\left(\begin{array}{cccccc|cccccc|cccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & - & 1 & - & 1 & - & 1 & - & 1 & - & 1 & - & 1 & - & 1 & - \\
1 & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - \\
\hline
1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 1 \\
\hline
1 & 1 & 1 & 1 & - & - & - & - & 1 & 1 & 1 & 1 & - & - & - & - \\
1 & - & 1 & - & - & 1 & - & 1 & 1 & - & 1 & - & - & 1 & - & 1 \\
\hline
1 & 1 & - & - & - & - & 1 & 1 & 1 & 1 & - & - & - & - & 1 & 1 \\
1 & - & - & 1 & - & 1 & 1 & - & 1 & - & - & 1 & - & 1 & 1 & - \\
\hline
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - \\
\hline
1 & - & 1 & - & 1 & - & 1 & - & - & 1 & - & 1 & - & 1 & - & 1 \\
\hline
1 & 1 & - & - & 1 & 1 & - & - & - & - & 1 & 1 & - & - & 1 & 1 \\
\hline
1 & - & - & 1 & 1 & - & - & 1 & - & 1 & 1 & - & - & 1 & 1 & - \\
1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - & 1 & 1 & 1 & 1 \\
1 & - & 1 & - & - & 1 & - & 1 & - & 1 & - & 1 & 1 & - & 1 & - \\
1 & 1 & - & - & - & - & 1 & 1 & - & - & 1 & 1 & 1 & 1 & - & - \\
1 & - & - & 1 & - & 1 & 1 & - & - & 1 & 1 & - & 1 & - & - & 1
\end{array}\right) \cdot \begin{pmatrix} 1 \\ - \\ - \\ 1 \\ - \\ - \\ 1 \\ 1 \\ - \\ 1 \\ - \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ -4 \\ -4 \\ 4 \\ -4 \\ -4 \\ 4 \\ 4 \\ -4 \\ 4 \\ -4 \\ 4 \\ 4 \\ 4 \\ 4 \\ 4 \end{pmatrix}$$

Boolean functions

A Boolean function f in n variables is any map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Its sign function is $F = (-1)^f$ and its Walsh-Hadamard transform (WHT) can be defined as

$$\widehat{F}(x) = \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)+x \cdot y} \in \mathbb{Z}$$

If H_n is the Hadamard matrix of Sylvester type of size 2^n, then

$$\widehat{F}^T = H_n F^T$$

Remark: We identify the functions F and $\widehat{F}$ with their Truth Tables.

Definition

The Boolean function f is said to be **bent** if all values of $\widehat{F}$ are equal to $\pm 2^{n/2}$.

Boolean functions

A Boolean function f in n variables is any map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Its sign function is $F = (-1)^f$ and its Walsh-Hadamard transform (WHT) can be defined as

$$\widehat{F}(x) = \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)+x\cdot y} \in \mathbb{Z}$$

If H_n is the Hadamard matrix of Sylvester type of size 2^n, then

$$\widehat{F}^T = H_n F^T$$

Remark: We identify the functions F and $\widehat{F}$ with their Truth Tables.

Definition

The bent function f is said to be

- **self-dual bent** if $F = (1/2^{n/2})\widehat{F}$, and
- **anti-self-dual bent** if $F = -(1/2^{n/2})\widehat{F}/2^{n/2}$.

Binary codes and Boolean functions

$$\overline{G}_k = (\overline{0}\ \ \overline{1}\ \ \overline{2}\ \cdots\ \overline{2^k - 1})$$

$$\overline{M}_k = \overline{G}_k^T \overline{G}_k$$

$$\overline{M}_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$1 \mapsto -1, \quad 0 \mapsto 1$$

Binary codes and Boolean functions

$$1 \mapsto -1, \quad 0 \mapsto 1$$

$$\overline{M}_3 \mapsto \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix} = H_3$$

$$\overline{M}_k \mapsto H_k$$

Binary codes and Boolean functions

Let χ be a characteristic vector of a projective binary code ($\chi \in \mathbb{F}_2^{2^k-1}$):

$$\chi \mapsto \overline{\chi} = (0, \chi) \in \mathbb{F}_2^{2^k}$$

$\Rightarrow$ $\overline{\chi}$ can be considered as a Truth Table of a Boolean function in k variables!

Conversely, if f is a Boolean function in k variables with $f(0) = 0$ then $f = (0, f')$, $f' \in \mathbb{F}_2^{2^k-1}$. We can consider f' as a characteristic vector of a binary projective linear code!

Binary codes and Boolean functions

If C is a self-polar binary code of

- length $n = 2^{2s-1} - 2^{s-1}$,
- dimension $k = 2s$,
- nonzero weights $w_1 = 2^{2s-2} - 2^{s-1}$ and $w_2 = 2^{2s-2}$,

it has n codewords of weight w_1. Some of its characteristic vectors give self-dual bent Boolean functions!

If C is a self-polar binary code of

- length $n = 2^{2s-1} + 2^{s-1}$,
- dimension $k = 2s$,
- nonzero weights $w_1 = 2^{2s-2} + 2^{s-1}$ and $w_2 = 2^{2s-2}$,

it has n codewords of weight w_1. Some of its characteristic vectors give anti-self-dual bent Boolean functions!

Computational results

Bouyukliev, Bouyuklieva, Dodunekov, On binary self-complementary $[120, 9, 56]$ codes having an automorphism of order 3 and associated SDP designs, 2007.

- There are exactly 4650 inequivalent self-complementary $[120, 9, 56]$ codes with nonzero weights 56, 64, and 120, which have an automorphism of order 3.
- From these codes we obtain 23284 inequivalent projective $[120, 8, 56]$ codes with nonzero weights 56 and 64.
- Exactly 3869 of them are self-polar
- These self-polar codes give 2559 self-dual bent function which are not CCZ-equivalent.