Orthogonal group and Boolean functions

Patrick Solé with M. Shi, L. Sok

CNRS/LAGA, University of Paris 8, 93 526 Saint-Denis, France ,
sole@enst.fr

BFA, Sosltrand, Norway

Outline

1. Around orthogonal group
2. Construction of self-dual codes
3. Construction of linear complementary dual codes
4. Generalized $\mathbb{Z}_{2^k}$ self-dual and regular bent functions

Orthogonal group over finite fields

The *orthogonal group* of index n over a finite field with q elements is defined by

$$\mathcal{O}_n(q) := \{A \in GL(n, q) | AA^T = I_n\}.$$

[Janusz] The orthogonal groups $\mathcal{O}_n := \mathcal{O}_n(2)$ are generated as follows

1. for $1 \leq n \leq 3$, $\mathcal{O}_n = \mathcal{P}_n$,
2. for $n \geq 4$, $\mathcal{O}_n = \langle \mathcal{P}_n, T_{\mathbf{u}} \rangle$,

where $\mathcal{P}_n$ is the permutation group of $n \times n$ matrices, $\mathbf{u}$ is a binary vector of Hamming weight 4 and $T_{\mathbf{u}}$ is the transvection defined by

$$\begin{aligned} T_{\mathbf{u}} : \quad & \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n \\ & \mathbf{x} \mapsto (\mathbf{x}.\mathbf{u})\mathbf{u}. \end{aligned}$$

Reference :

[1] G. J. Janusz, "Parametrization of self-dual codes by orthogonal matrices," *Finite Fields Appl.*, Vol. 13, No. 3,(2007) 450–491.

Notation and Definitions

Let $q = p^m$ for some prime p and some positive integer m. Let $\theta = \frac{p-1}{2} \in \mathbb{F}_p$ if $p \neq 2$ and $\theta = 1$ otherwise. Let $\alpha, \beta \in \mathbb{F}_q \backslash \{0\}$ such that $\alpha^2 + \beta^2 = 1$ and $\mathbf{v} = (\alpha - 1)\mathbf{e}_1 + \beta\mathbf{e}_2, \mathbf{w} = -\beta\mathbf{e}_1 + (\alpha - 1)\mathbf{e}_2$. Let $\mathbf{u} = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4$ if $n \geq 4$, where $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ is the canonical basis of $\mathbb{F}_q^n$. Define two linear maps

$$T_{\mathbf{u},\theta} : \begin{array}{l} \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n, \\ \mathbf{x} \mapsto \theta(\mathbf{x}.\mathbf{u})\mathbf{u} \end{array} \qquad T_{\alpha,\beta} : \begin{array}{l} \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n \\ \mathbf{x} \mapsto \mathbf{x} + (\mathbf{x}.\mathbf{v})\mathbf{e}_1 + (\mathbf{x}.\mathbf{w})\mathbf{e}_2. \end{array}$$

Denote

$$\mathcal{T}_n(q) := \begin{cases} \langle \mathcal{P}_n, T_{\alpha,\beta} \rangle & \text{if } n \leq 3, \\ \langle \mathcal{P}_n, T_{\alpha,\beta}, T_{\mathbf{u},\theta} \rangle, & \text{otherwise.} \end{cases}$$

TABLE: Orders $|\mathcal{T}_n(q)|$ and $|\mathcal{O}_n(q)|$ for $3 \le q \le 16$, $n = 4, 5$

q	$\lvert\mathcal{T}_4(q)\rvert$[1]	$\lvert\mathcal{O}_4(q)\rvert$[2]	$\lvert\mathcal{T}_5(q)\rvert$[1]	$\lvert\mathcal{O}_5(q)\rvert$[2]
3	384	1152	103680	103680
4	3840	3840	979200	979200
5	384	28800	18720000	18720000
7	225792	225792	553190400	553190400
8	258048	258048	1056706560	1056706560
9	1036800	1036800	6886425600	6886425600
11	3484800	3484800	51442617600	51442617600
13	9539712	9539712	274075925760	274075925760
16	16711680	16711680	1095199948800	1095199948800

References :

[1] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Sydney, 1995.

[2] F. MacWilliams, "Orthogonal matrices over finite fields," Amer. Math. Monthly 76 (1969) 152–164.

Generation of $\mathcal{O}_n(q)$

- $\mathcal{O}_n(3) = \langle \mathcal{P}_n, T_{\mathbf{u},\theta} \rangle$ for $n \geq 6$.
- Conjecture : for $q > 3, \mathcal{O}_n(q) = \langle \mathcal{P}_n, T_{\alpha,\beta}, T_{\mathbf{u},\theta} \rangle = \mathcal{T}_n(q)$ for $n \geq 4$.

Linear codes

- An $[n, k]$ code over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$.
- The distance of $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_q^n$ is $d(\mathbf{x}, \mathbf{y}) := |\{i : x_i \neq y_i\}|$.
- An $[n, k]$ code with minimum distance d is denoted by $[n, k, d]$ code
- The *dual* of C is $C^\perp := \{x \in \mathbb{F}_q^n : x.y := \sum_{i=1}^n x_i y_i = 0\}$.
- A linear code C is called *self-orthogonal* if $C \subset C^\perp$ and *self-dual* if $C = C^\perp$.
- A linear code C is called *linear complementary dual* (LCD) if $C \cap C^\perp = \{0\}$
- An $[n, k, d]$ code is called *Maximum Distance Separable* (MDS) if

$$d = n - k + 1$$

Fact

Let C be a linear code of length n over $\mathbb{F}_q$ with its parity check matrix written in the systematic form

$$H = \left(\begin{array}{c|c} I_n & A \end{array} \right),$$

where I_n is the identity matrix and A is a square matrix of index n. Then

C is self-dual if and only if $AA^T = -I_n$.

First construction

Let $q \equiv 1 \pmod 4$. Fix $\alpha \in \mathbb{F}_q$ such that $\alpha^2 \equiv -1 \pmod q$. Then a matrix G_n of the following form :

$$G_n = \left(\begin{array}{c|c} I_n & \alpha L \end{array} \right), \tag{1}$$

where $L \in \mathcal{O}_n(q)$, generates a self-dual $[2n, n]$ code.

First construction continued

Let $q \equiv 3 \pmod 4$. Fix $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha^2 + \beta^2 \equiv -1 \pmod q$ and $D_0 = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$. Then a matrix G_n of the following form :

$$G_n = \left(\begin{array}{c|c} I_{2n} & D_n L \end{array} \right), \tag{2}$$

where $L \in \mathcal{O}_{2n}(q), D_n = I_n \otimes D_0$, generates a self-dual $[4n, 2n]$ code.

Second construction

Let $q \equiv 1 \pmod 4$. Let C_n be a self-dual code $[2n, n, d]$ over $\mathbb{F}_q$ with its generator matrix G_n. Fix $a, b \in \mathbb{F}_q$ such that $a^2 + b^2 \equiv 0 \pmod q$. Then for any $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_q$, an extended code $\bar{C}_n$ of C_n with the following generator matrix $G_{\bar{C}_n}$ is a self-orthogonal $[2n+2, n, \geq d]$ code :

$$G_{\bar{C}_n} = \begin{pmatrix} & \lambda_1 a & \lambda_1 b \\ & \lambda_2(-b) & \lambda_2 a \\ & \vdots & \vdots \\ G_n & \lambda_{2i-1} a & \lambda_{2i-1} b \\ & \lambda_{2i}(-b) & \lambda_{2i} a \\ & \vdots & \vdots \end{pmatrix}. \qquad (3)$$

Second construction continued

Let $q \equiv 1 \pmod 4$. Let C_n be a self-dual code $[2n, n, d]$ over $\mathbb{F}_q$ with its generator matrix $(I_n|A)$. Fix $a, b, c, d \in \mathbb{F}_q$ such that $a^2 + b^2 \equiv c^2 + d^2 \equiv 0 \pmod q$. Let x be a vector of length $n+2$ orthogonal to all extended rows of A such that $x.x \equiv 0 \pmod q$. Then for any $\lambda_1, \ldots, \lambda_{n+1} \in \mathbb{F}_q$, a code C'_n with the following generator matrix is a self-orthogonal $[2n+4, n+1]$ code :

$$\left(\begin{array}{ccc|c cc|cc} & & & & \lambda_1 a & \lambda_1 b & \lambda_1 c & \lambda_1 d \\ & & & & \lambda_2(-b) & \lambda_2 a & \lambda_2(-d) & \lambda_2 c \\ & I_n & & A & & \vdots & \vdots & \vdots \\ & & & & \lambda_{2i-1} a & \lambda_{2i-1} b & \lambda_{2i-1} c & \lambda_{2i-1} d \\ & & & & \lambda_{2i}(-b) & \lambda_{2i} a & \lambda_{2i}(-d) & \lambda_{2i} c \\ & & & & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & & x & & \lambda_{n+1} d & \lambda_{n+1}(-c) \end{array}\right). \tag{4}$$

Numerical results

TABLE: Optimal and Best known self-dual codes, M : MDS, A : almost MDS, * : new parameters

2n/q	**3**	**5**	**7**	**11**	**13**	**17**	**19**	**23**	**29**	**31**	**37**	**41**	**43**	**47**
4	*M*	*A*	*M*	*M*	*M*	*M*	*M*	*M*	*M*	*M*	*M*	*M*	*M*	*M*
6		*M*			*M*	*M*			*M*		*M*	*M*		
8			*M*	*M*	*M*	*M*	*M*	*M*	*M*	*M*	*M*	*M*	*M*	*M*
10					*M*	*M*			*M*		*M*	*M*		
12		*A*	*A*	*M*	*A*	6	*M*	*M*	*M*	*M*	*M*	*M*	*M*	*M*
14					7	7					7			
16						8	8		8	8	8	8	8	8

Numerical results

TABLE: Optimal and Best known self-dual codes, M : MDS, A : almost MDS, * : new parameters

2n/q	53	59	61	67	71	73	79	83	89	97	101	103
4	M^*	M^*	M^*	M^*	M^*	M^*	M	M^*	M^*	M	M^*	M^*
6	M		M			M			M^*	M^*	M^*	
8	M^*	M^*	M^*	M^*	M^*	M^*	M^*	M^*	M^*	M^*	M^*	M^*
10	M^*		M^*			M^*			M^*	M^*	M^*	M^*
12	M^*	M^*	M^*	M^*	M^*	M^*	M^*	M^*	M^*	M^*	M^*	M^*

Characterization of LCD codes

[Dougherty et al.] Let $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ be vectors over a commutative ring R such that $\mathbf{u}_i.\mathbf{u}_i = 1$ for each i and $\mathbf{u}_i.\mathbf{u}_j = 0$ for $i \neq j$. Then $C = \langle \mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \rangle$ is an LCD code over R.

[Massey] Let G be a generator matrix for a code over a field. Then $det(GG^\top) \neq 0$ if and only if G generates an LCD code.

References :

[1] S. T. Dougherty, J-L. Kim, B. Ozkaya , L. Sok and P. Sole," The combinatorics of LCD codes : Linear Programming bound and orthogonal matrices," International Journal of Information and Coding Theory, to appear

[2] J.L. Massey, Linear codes with complementary duals, Discrete Mathematics, 106–107, 337–342, 1992.

Construction of LCD codes from orthogonal matrices

Let $A \in \mathcal{O}_n(q)$ and A_k a submatrix obtained from A by keeping k rows. Then the matrix

$$G = A_k \tag{5}$$

generates an LCD code.

Construction of LCD codes from orthogonal matrices

Let $A \in \mathcal{O}_n(q)$ and A_k a submatrix obtained from A by keeping k rows. Then for any $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_q \backslash \{0\}$, the matrix

$$G = diag(\lambda_1, \ldots, \lambda_k)A_k \tag{6}$$

generates an LCD code.

Recursive construction

Let C_n be an LCD code $[n, k, d]$ over $\mathbb{F}_q$ with its generator matrix G_n being rows of an orthogonal matrix. Assume that there exist $a, b \in \mathbb{F}_q \backslash \{0\}$ such that $a^2 + b^2 \equiv 0 \pmod{q}$. Then for any $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_q$, an extended code $\bar{C}_n$ of C_n with the following generator matrix $G_{\bar{C}_n}$ is an LCD code $[n+2, k, \geq d]$:

$$G_{\bar{C}_n} = \left(\begin{array}{c|cc} & \lambda_1 a & \lambda_1 b \\ & \lambda_2(-b) & \lambda_2 a \\ & \vdots & \vdots \\ G_n & & \\ & \lambda_{2i-1} a & \lambda_{2i-1} b \\ & \lambda_{2i}(-b) & \lambda_{2i} a \\ & \vdots & \vdots \end{array} \right). \tag{7}$$

Matrix product LCD codes

Recall that the matrix-product code $C = [C_1, \ldots, C_l]A$ is a linear code whose all codewords are matrix product $[c_1, \ldots, c_l]A$, where $c_i \in C_i$ is an $n \times 1$ column vector and $A = (a_{ij})_{l \times m}$ is an $l \times m$ matrix over $\mathbb{F}_q$. Here $l \leq m$ and C_i is an $[n, k_i, d_i]_{\mathbb{F}_q}$ code over $\mathbb{F}_q$. If $C_1, \ldots, C_l$ are linear with generator matrices $G_1, \ldots, G_l$, respectively, then $[C_1, \ldots, C_l]A$ is linear with generator matrix

$$G = \begin{pmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1m}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2m}G_2 \\ \vdots & \vdots & \cdots & \vdots \\ a_{l1}G_l & a_{l2}G_l & \cdots & a_{lm}G_l \end{pmatrix}.$$

Some known results

- Let $(C_i)_{1\leq i\leq l}$ be linear codes over F_q with parameters $[n, k_i]$ and A be an $l \times m$ matrix of full row rank. Then $C = [C_1, \ldots, C_l]A$ is an $[mn, \sum_{i=1}^{l} k_i]$ code.
- Let $(C_i)_{1\leq i\leq l}$ be linear codes over F_q with parameters $[n, k_i]$ and A be a non-singular matrix. If $C = [C_1, \ldots, C_l]A$, then $([C_1, \ldots, C_l]A)^{\perp} = [C_1^{\perp}, \ldots, C_l^{\perp}](A^{-1})^{\top}$.

Characterization of matrix product LCD codes

Let $C_1, C_2, \ldots, C_l$ be linear codes over $\mathbb{F}_q$. Let $A \in \mathcal{O}_l(q)$ and $\bar{A} = diag(a_1, \ldots, a_l)A$ with $a_1, \ldots, a_l \in \mathbb{F}_q \setminus \{0\}$. Then $C = [C_1, C_2, \ldots, C_l]\bar{A}$ is a matrix product LCD code if and only if $C_1, C_2, \ldots, C_l$ are all LCD codes.

Projection over self-dual basis

Let $B = \{e_0, e_1, \cdots, e_{\ell-1}\}$ be a self-dual basis of $\mathbb{F}_{q^\ell}$ over $\mathbb{F}_q$, that is,

$$\mathrm{Tr}(\mathrm{e_i}, \mathrm{e_j}) = \delta_{\mathrm{i,j}},$$

where Tr denotes the trace of $\mathbb{F}_{q^\ell}$ down to $\mathbb{F}_q$ and $\delta_{i,j}$ is the Kronecker symbol. Define

$$\phi_B : \mathbb{F}_{q^\ell} \longrightarrow \mathbb{F}_q^\ell, \sum_{i=0}^{\ell-1} a_i e_i \mapsto (a_0, \ldots, a_{\ell-1}),$$

and extend ϕ to $\mathbb{F}_{q^\ell}^n$ in the natural way. Then
A linear code C of length n over $\mathbb{F}_{q^\ell}$ is LCD if and only if the linear code $\phi_B(C)$ of length $n\ell$ over $\mathbb{F}_q$ is LCD.

LCD codes from self-orthogonal codes

Assume that there exists an MDS self-orthogonal $[n, k]$ code over $\mathbb{F}_q$. Then there exists an MDS LCD $[n-k, k']$ code for $1 \leq k' \leq k$.

Existence of MDS LCD codes

1. For any even prime power $q = 2^m$, there exists an MDS LCD $[n, k]$ code for $1 \leq n \leq 2^{m-1}, 1 \leq k \leq n$.
2. For any odd prime power q there exists an MDS LCD $[n, k]$ code, for $1 \leq k \leq n$, with the following conditions.
    1. $n = (q+1)/2$,
    2. $q \equiv 1 \pmod 4$ $q \geq 2^{(2n)} \times (2n)^2$,
    3. $q = r^2$ and $2n \leq r$,
    4. $q = r^2$ and $2n - 1$ is an odd divisor of $q - 1$,
    5. $r \equiv 3 \pmod 4$ and $n = tr$ for any $t \leq (q-1)/2$.

References :

[1] M. Grassl and T. A. Gulliver, "On Self-Dual MDS Codes" *ISIT 2008*, Toronto, Canada, July 6 –11, 2008

[2] L. F. Jin and C. P. Xing, New MDS self-dual codes from generalized Reed-Solomon codes, arXiv :1601.04467v1, 2016.

More existence of MDS LCD codes

Let $q = p^m, m > 1$ for some prime p, $n|q-1$ and $k \leq \lfloor (n-1)/2 \rfloor$. Then there exists an MDS LCD $[n-k, k']$ code for $1 \leq k' \leq k$.

Optimal LCD codes from random sampling

Over $\mathbb{F}_4$	Over $\mathbb{F}_7$	Over $\mathbb{F}_{11}$	Over $\mathbb{F}_{25}$
$[8,2,6]_{\mathbb{F}_4}$	$[8,2,7]_{\mathbb{F}_7}$	$[8,2,7]_{\mathbb{F}_{11}}$	$[8,2,7]_{\mathbb{F}_{25}}$
$[8,3,5]_{\mathbb{F}_4}$	$[8,3,6]_{\mathbb{F}_7}$	$[8,3,6]_{\mathbb{F}_{11}}$	$[8,3,6]_{\mathbb{F}_{25}}$
$[8,4,4]_{\mathbb{F}_4}$	$[8,4,5]_{\mathbb{F}_7}$	$[8,4,5]_{\mathbb{F}_{11}}$	$[8,4,5]_{\mathbb{F}_{25}}$
$[8,5,3]_{\mathbb{F}_4}$	$[8,5,4]_{\mathbb{F}_7}$	$[8,5,4]_{\mathbb{F}_{11}}$	$[8,5,4]_{\mathbb{F}_{25}}$
$[8,6,2]_{\mathbb{F}_4}$	$[8,6,3]_{\mathbb{F}_7}$	$[8,6,3]_{\mathbb{F}_{11}}$	$[8,6,3]_{\mathbb{F}_{25}}$
$[8,7,2]_{\mathbb{F}_4}$	$[8,7,2]_{\mathbb{F}_7}$	$[8,7,2]_{\mathbb{F}_{11}}$	$[8,7,2]_{\mathbb{F}_{25}}$
$[9,2,7]_{\mathbb{F}_4}$	$[9,2,7]_{\mathbb{F}_7}$	$[9,2,8]_{\mathbb{F}_{11}}$	$[9,2,8]_{\mathbb{F}_{25}}$
$[9,3,6]_{\mathbb{F}_4}$	$[9,3,6]_{\mathbb{F}_7}$	$[9,3,7]_{\mathbb{F}_{11}}$	$[9,3,7]_{\mathbb{F}_{25}}$
$[9,4,5]_{\mathbb{F}_4}$	$[9,4,5]_{\mathbb{F}_7}$	$[9,4,\geq 5]_{\mathbb{F}_{11}}$	$[9,4,6]_{\mathbb{F}_{25}}$

Optimal LCD code from projection over self-dual basis

Over $\mathbb{F}_4$	Over $\mathbb{F}_2$	Over $\mathbb{F}_8$	Over $\mathbb{F}_2$
$[12, 2, 9]_{\mathbb{F}_4}$	$[24, 4, \geq 11]_{\mathbb{F}_2}$	$[7, 4, 4]_{\mathbb{F}_8}$	$[21, 12, \geq 4]_{\mathbb{F}_2}$
$[12, 3, 8]_{\mathbb{F}_4}$	$[24, 6, \geq 9]_{\mathbb{F}_2}$	$[7, 5, 3]_{\mathbb{F}_8}$	$[21, 15, \geq 3]_{\mathbb{F}_2}$
$[12, 4, 7]_{\mathbb{F}_4}$	$[24, 8, 8]_{\mathbb{F}_2}$	$[8, 1, 8]_{\mathbb{F}_8}$	$[24, 3, 13]_{\mathbb{F}_2}$
$[12, 8, 4]_{\mathbb{F}_4}$	$[24, 16, 4]_{\mathbb{F}_2}$	$[8, 2, 7]_{\mathbb{F}_8}$	$[24, 6, \geq 9]_{\mathbb{F}_2}$
$[12, 9, 2]_{\mathbb{F}_4}$	$[24, 18, \geq 3]_{\mathbb{F}_2}$	$[8, 5, 4]_{\mathbb{F}_8}$	$[24, 15, 4]_{\mathbb{F}_2}$

Over $\mathbb{F}_{27}$	Over $\mathbb{F}_3$	Over $\mathbb{F}_{2^m}$	Over $\mathbb{F}_2$
$[5, 1, 5]_{\mathbb{F}_{27}}$	$[15, 3, 9]_{\mathbb{F}_3}$	$[5, 3, 3]_{\mathbb{F}_{2^7}}$	$[35, 21, \geq 5]_{\mathbb{F}_2}$
$[5, 2, 4]_{\mathbb{F}_{27}}$	$[15, 6, \geq 6]_{\mathbb{F}_3}$	$[6, 5, 2]_{\mathbb{F}_{2^7}}$	$[42, 35, \geq 3]_{\mathbb{F}_2}$
$[5, 3, 3]_{\mathbb{F}_{27}}$	$[15, 9, 4]_{\mathbb{F}_3}$	$[6, 5, 2]_{\mathbb{F}_{2^8}}$	$[48, 40, \geq 3]_{\mathbb{F}_2}$
$[6, 1, 6]_{\mathbb{F}_{27}}$	$[18, 3, \geq 11]_{\mathbb{F}_3}$	$[6, 5, 2]_{\mathbb{F}_{2^9}}$	$[54, 45, \geq 3]_{\mathbb{F}_2}$
$[6, 2, 5]_{\mathbb{F}_{27}}$	$[18, 6, \geq 8]_{\mathbb{F}_3}$	$[6, 5, 2]_{\mathbb{F}_{2^{10}}}$	$[60, 50, \geq 3]_{\mathbb{F}_2}$
$[6, 3, 4]_{\mathbb{F}_{27}}$	$[18, 9, 6]_{\mathbb{F}_3}$	$[6, 5, 2]_{\mathbb{F}_{2^{12}}}$	$[72, 60, \geq 3]_{\mathbb{F}_2}$
$[6, 4, 3]_{\mathbb{F}_{27}}$	$[18, 12, 4]_{\mathbb{F}_3}$		

Commercial Break

PURE AND APPLIED MATHEMATICS
Edited by Dominique Perrin

Codes and Rings

Theory and Practice

Codes and Rings is a systematic review of the literature focusing on codes over rings and rings acting on codes. Since the breakthrough works on quaternary codes in the 1990s, two decades of research have moved the field far beyond its original periphery. This book fills this gap by consolidating results scattered in the literature, addressing classical as well as applied aspects of rings and coding theory. New research covered by the book encompasses skew cyclic codes, decomposition theory of quasi-cyclic codes and related codes, and MDS convolutional codes over rings. Primarily suitable for ring theorists at the PhD level engaged in application research, and coding theorists interested in algebraic foundations, the work is also valuable to computational scientists and working cryptologists in the area.

Key Features

- Consolidates 20+ years of research in one volume, helping researchers save time in the evaluation of a disparate literature.
- Reviews decomposition of quasi-cyclic codes under ring action.
- Evaluates the ideal and module structure of skew-cyclic codes.
- Supports applications in data compression, space time coding, code division multiple access, spread spectrum, and PAPR reduction.

About the Authors

Minjia Shi is an Associate Professor of Mathematics in the School of Mathematical Sciences of Anhui University, P. R. China since 2012. He is the author of more than 60 journal articles and one book. He is interested in algebraic coding, cryptography, and related fields.

Adel Alahmadi is an Associate Professor of Mathematics at King Abdulaziz University, Jeddah, Saudi Arabia. He is interested in algebraic geometry and ring theory.

Patrick Solé is a Research Professor at Centre National de la Recherche Scientique since 1996. His research interests include coding theory (covering radius, codes over rings, geometric codes, quantum codes) and cryptography (Boolean functions). He is the author of more than 150 journal articles and two books.

ELSEVIER
ACADEMIC PRESS
An imprint of Elsevier
elsevier.com

ISBN 978-0-12-813388-0
9 780128 133880

Perrin
PURE AND APPLIED MATHEMATICS
Codes and Rings
Shi
Alahmadi
Solé
ACADEMIC PRESS

PURE AND APPLIED MATHEMATICS
Edited by Dominique Perrin

Codes and Rings
Theory and Practice

Minjia Shi
Adel Alahmadi
Patrick Solé

$\mathbb{Z}_4-$bent functions

- A generalized Boolean function $f : \mathbb{F}_2^n \mapsto \mathbb{Z}_q$, for q integer.
- For $q = 4$, the set of all such functions will be denoted by $\mathcal{Q}_n$.
- The (complex) sign function of f is $F(x) := (i)^{f(x)}$.
- The quaternary Walsh-Hadamard transform $H_f(u)$ of f is $H_f(u) := \sum_{x\in\mathbb{F}_2^n}(-1)^{x\cdot u}F(x)$. In matrix terms $H_f(u) = H_n F$.
- A function $f \in \mathcal{Q}_n$, is bent if $|H_f(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$.
- A bent quaternary function is said to be regular if there is an element $\widehat{f}$ of $\mathcal{Q}_n$, such that its sign function satisfies $H_f(u) = 2^{n/2}\tilde{F}$.
- If, furthermore, $f = \widehat{f}$, then f is self-dual bent . Similarly, if $f = \widehat{f} + 2$ then f is anti self-dual bent .

$\mathbb{Z}_4-$Reed-Mueller codes

There are two quaternary generalizations of Reed-Mueller codes in Hammons et al.
The codes $QRM(r, m)$ are obtained by Hensel lifting from the binary Reed-Mueller codes.
The codes $ZRM(r, m)$ are obtained by a multilevel construction from the RM codes. Symbolically,
$ZRM(r, m) = RM(r - 1, m) + 2RM(r, m)$.
We require a third one, introduced in Davis and Jedwab.
Consider codes of length 2^m, generated by evaluations of quaternary Boolean functions on the 2^m points of $\mathbb{F}_2^m$. The code $RM_4(r, m)$ is generated by the monomials of order at most r. It contains $4^{\sum_{j=0}^{r} \binom{m}{j}}$ codewords and has both Hamming and Lee distance equal to 2^{m-r}
As pointed out in Borges et al. (2008),
$RM_4(r, m) = ZRM(r + 1, m)$, for $r \leq m - 1$.

Pairs of SD bent functions vs SD $\mathbb{Z}_4-$ bent functions

Assume $F = a + bi$ is the sign function of a quaternary self-dual bent function, with a, b reals. There is a pair of binary self-dual bent functions given by their sign functions G, H as

$$\begin{aligned} G &= a + b, \\ K &= a - b. \end{aligned}$$

Conversely, every pair G, H of binary self-dual bent functions produces a quaternary self-dual bent function in that way.
$\Rightarrow$ There is no self-dual or anti-self-dual bent quaternary Boolean function in odd number of variables.

Pairs of regular bent functions vs regular $\mathbb{Z}_4-$bent function

Assume $F = a + bi$ is the sign function of a regular quaternary bent function, with a, b reals. There is a pair of binary bent functions g, k given by their sign functions G, H as

$$\begin{aligned} G &= a + b, \\ K &= a - b. \end{aligned}$$

Conversely, every pair g, k of binary bent functions produces a regular quaternary bent function in that way.
$\Rightarrow$There is no regular bent quaternary Boolean function in odd number of variables.

Connection with the Gray map

A connection with the Gray map of Hammons et al. 1994 is established as follows.
Assume that $f = r + 2s$ is quaternary Boolean function with r, s Boolean functions. Then $g = s$, and $k = r + s$.

Maiorana-McFarland type

A general class of quaternary bent functions is the following quaternary analogue of the so-called Maiorana-McFarland class. Consider all functions of the form

$$2x \cdot \phi(y) + g(y)$$

with x, y dimension $n/2$ variable vectors, ϕ any permutation in $\mathbb{F}_2^{n/2}$, and g arbitrary quaternary Boolean. In the following theorem, we consider the case where $\phi \in GL(n/2, 2)$.

Maiorana-McFarland type ct'd

A Maiorana-McFarland function is self-dual bent (resp. anti self-dual bent) if $g(y) = b \cdot y + \epsilon$ and $\phi(y) = L(y) + a$ where L is a linear automorphism satisfying $L \times L^t = I_{n/2}$, $a = L(b)$, and a has even (resp. odd) Hamming weight.
The code of parity check matrix $(I_{n/2}, L)$ is self-dual and (a, b) one of its codewords. Conversely, to the ordered pair (H, c) of a parity check matrix H of a self-dual code of length n and one of its codewords c can be attached such a Boolean function.

Dillon function type

As usual, make the convention that $\frac{1}{0} = 0$.
Assume G_0 and G_1 to be balanced Boolean function of m variables, with $G_0(0) = G_1(0) = 0$, and satisfying $\sum_{t \in \mathbb{F}_{2^m}} i^{G_0(t)+2G_1(t)} = 0$.
The quaternary Boolean function f in $2m$ variables defined by

$$f(x, y) = G_0(x/y) + 2G_1(x/y)$$

is bent with dual

$$\widehat{f}(x, y) = G_0(y/x) + 2G_1(y/x).$$

Algorithms I

Theorem Let $n \geq 2$ be an even integer and Z be arbitrary in $\{\pm 1, \pm i\}^{2^{n-1}}$. Define $Y := Z + \frac{2H_{n-1}}{2^{n/2}}Z$. If Y is in $\{\pm 1, \pm i\}^{2^{n-1}}$, then the vector (Y, Z) is the sign function of a self-dual bent function in n variables. Moreover all self-dual bent functions respect this decomposition.

Gives a search algorithm called $SDB(n, k)$
to compute all self dual quaternary bent Boolean function of degree at most k in n variables,
analogous algorithm $ASDB(n, k)$ for quaternary anti-self-dual bent Boolean function in n variables, of degree at most k.

Algorithms II

Algorithm $SDB(n,k)$

1. Generate all $Z = i^z$ with z in $RM_4(k, n-1)$.
2. Compute all Y as $Y := Z + \frac{2H_{n-1}}{2^{n/2}} Z$.
3. If $Y \in \{\pm 1, \pm i\}^{2^{n-1}}$ output (Y, Z), else go to next Z.

Similarly **Algorithm** $ASDB(n,k)$

1. Generate all $Z = i^z$ with z in $RM_4(k, n-1)$.
2. Compute all Y as $Y := Z - \frac{2H_{n-1}}{2^{n/2}} Z$.
3. If $Y \in \{\pm 1, \pm i\}^{2^{n-1}}$ output (Y, Z), else go to next Z.

Complexity

To show the memory space savings with comparison with the brute force exhaustive search of complexity 4^{2^n}, the search space is only of the size of the Reed-Muller code that is $2^{2(\sum_{j=0}^{k}\binom{n-1}{j})}$.

Numerics

We classify quaternary self-dual bent functions under the extended orthogonal group. Recall that two $n-$variable functions f and f' are equivalent if for any $x \in \mathbb{F}_2^n$, $f'(x) = f(Lx) + c$ for some $L \in \mathcal{O}_n, c \in \mathbb{Z}_4$.

We give the complete classification for all the functions in two and four variables ,

the Gray image (the ordered pair (g, k) above) of their equivalence classes

and the classification of all quadratic functions in six variables .

In accordance with our theory, the total number of quaternary self-dual bent functions is the square of that of self-dual bent functions in Carlet et al., namely 2^2 in the case of two variables, and 20^2 in the case of four variables.

Classification method

Classification :

1. Searching all the functions using Algorithm $SDB(n, k)$
2. Rejecting isomorphism under extended orthogonal group $\mathcal{O}_n$

Result : There are 1, 8 non-equivalent quaternary self-dual bent functions in 2, 4 variables respectively and 45 non-equivalent quadratic self-dual bent functions in 6 variables.

$\Rightarrow$ classification of quaternary self-dual bent functions of degree four in eight variables is intractable in practice (too many orbits).

Numerical results

TABLE: Quaternary self-dual bent functions in 2 and 4 variables

Representative from equivalence class	Size
2 2 2 0	4
Number of quaternary self-dual bent functions in two variables	4

Representative from equivalence class	Size
0 2 2 0 2 0 2 0 2 2 0 0 0 0 0 0	24
2 0 2 2 2 2 0 2 2 2 0 2 0 2 0 0	16
0 3 3 0 3 1 3 1 3 3 1 1 0 1 1 0	48
0 3 3 0 3 0 2 1 3 2 0 1 0 1 1 0	24
3 1 2 3 2 3 1 3 2 2 0 3 0 3 0 0	96
1 3 2 1 2 1 3 1 2 2 0 1 0 1 0 0	96
2 1 2 3 2 3 0 3 3 2 1 2 1 2 1 0	48
0 2 2 0 2 1 3 0 2 3 1 0 0 0 0 0	48
Number of quaternary self-dual bent functions in four variables	400

Numerical results cont'

TABLE: Gray image $(s, r+s)$ of the equivalence classes

Binary self-dual bent function g	Binary self-dual bent function k
1 1 1 0	1 1 1 0
0 1 1 0 1 0 1 0 1 1 0 0 0 0 0 0	0 1 1 0 1 0 1 0 1 1 0 0 0 0 0 0
1 0 1 1 1 1 0 1 1 1 0 1 0 1 0 0	1 0 1 1 1 1 0 1 1 1 0 1 0 1 0 0
0 1 1 0 1 0 1 0 1 1 0 0 0 0 0 0	0 0 0 0 0 1 0 1 0 0 1 1 0 1 1 0
0 1 1 0 1 0 1 0 1 1 0 0 0 0 0 0	0 0 0 0 0 0 1 1 0 1 0 1 0 1 1 0
1 0 1 1 1 1 0 1 1 1 0 1 0 1 0 0	0 1 1 0 1 0 1 0 1 1 0 0 0 0 0 0
0 1 1 0 1 0 1 0 1 1 0 0 0 0 0 0	1 0 1 1 1 1 0 1 1 1 0 1 0 1 0 0
1 0 1 1 1 1 0 1 1 1 0 1 0 1 0 0	1 1 1 0 1 0 0 0 0 1 1 1 1 1 1 0
0 1 1 0 1 0 1 0 1 1 0 0 0 0 0 0	0 1 1 0 1 1 0 0 1 0 1 0 0 0 0 0

$\mathbb{Z}_{2^m}$ generalized Boolean functions

- A *generalized Boolean function* (gBF) $f : \mathbb{F}_2^n \mapsto \mathbb{Z}_q$, for integer q integer. In this work $q = 2^m$, for some integer $m > 1$.The set of all such gBFs will be denoted by $\mathcal{GB}_n$.
- The (complex) *sign function* of f is $F(x) := (\omega)^{f(x)}$, where ω stands for a complex root of unity of order 2^m.
- The *Walsh-Hadamard* transform $H_f(u)$ of the Boolean function f, evaluated in a point u of the domain $\mathbb{F}_2^n$, is defined as $H_f(u) = \sum_{x\in\mathbb{F}_2^n}(-1)^{x.u}F(x)$. In matrix terms $H_f(u) = H_nF$.
- A function $f \in \mathcal{GB}_n$, is said to be *bent* if $|H_f(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$.
- A bent gBF is said to be *regular* if there is an element $\widehat{f}$ of $\mathcal{GB}_n$, such that its sign function satisfies $H_f(u) = 2^{n/2}\widehat{f}$.
- If, furthermore, $f = \widehat{f}$, then f is *self-dual bent* . Similarly, if $f = \widehat{f} + 2^{m-1}$, then f is *anti-self-dual bent* .

Definition

Definition : A system of 2^s boolean functions $f_0, \cdots, f_{2^s-1}$, with respective sign functions $F_0, \cdots, F_{2^s-1}$, is said to have the *Hadamard property* if

$$H_s(F_0, \cdots, F_{2^s-1})^\top$$

is equal to $\pm$ some column of H_s.

$\mathbb{Z}_{2^m}-$ regular bent gBF functions

If the sign function of the regular bent gBF f is $\omega^f = \sum_{i=0}^{k-1} a_i\omega^i$, then the k BF G_i for $i = 0, \cdots, k-1$ defined by

$$(G_0, \cdots, G_{k-1})^\top = H_{m-1}(a_0, \cdots, a_{k-1})^\top$$

are bent BF with the Hadamard property, and so is the system of their duals. Conversely, given k BF $G_0, \cdots, G_{k-1}$, with the Hadamard property, with duals also with Hadamard property, the gBF of sign function $\sum_{i=0}^{k-1} a_i\omega^i$ with the a_i's are defined by the above system is regular bent.
$\Rightarrow$ There is no regular bent $\mathbb{Z}_{2^m}$-valued gBF in odd number of variables.

$\mathbb{Z}_{2^m}-$ self-dual bent gBF functions

If the sign function of the self-dual bent gBF f is $\omega^f = \sum_{i=0}^{k-1} a_i \omega^i$, then the k self-dual BFs G_i for $i = 0, \cdots, k-1$ defined by

$$(G_0, \cdots, G_{k-1})^\top = H_{m-1}(a_0, \cdots, a_{k-1})^\top$$

are bent BF with the Hadamard property. Conversely, given k BF $G_0, \cdots, G_{k-1}$, with the Hadamard property,the gBF of sign function $\sum_{i=0}^{k-1} a_i \omega^i$ where the a_i's are defined by the above system is self-dual bent.

$\Rightarrow$ There is no self-dual bent $\mathbb{Z}_{2^m}$-valued gBF in odd number of variables.

Symmetries

Let f be a quaternary regular bent function in n variables. Then $g(x) = f(xM + a) + c$, where $M \in GL(n, 2)$, $a \in \mathbb{F}_2^n$ and $c \in \mathbb{Z}_4$ is also regular bent.

Classification of quaternary regular bent functions

By applying our decomposition technique, we can now classify all quaternary regular bent functions upto four variables.

Result : Up to affine equivalence, there are $2, 7$ non-equivalent quaternary regular bent functions in $2, 4$. The number of quaternary reqular bent functions is the square of that of binary case and more precisely there are $8^2, 896^2, (3502 \times 13888)^2$ in $2, 4, 6$ variables respectively.

Numerical results

TABLE: Quaternary regularbent functions in two and four variables

Representative from equivalence class	*Size*
2101	16
2000	48
Number of quaternary regular bent functions in two variables	64
2000202220000200	1792
3100312231111311	80640
2101202230010211	129024
3001202231000301	215040
3100303221011300	322560
2101212321010301	26880
2011202220000211	26880
Number of quaternary regular bent functions in four variables	802816

Thank you very much for your attention