Construction of self-orthogonal $\mathbb{Z}_{2^k}$-codes

Sara Ban

sban@math.uniri.hr

Faculty of Mathematics, University of Rijeka, Croatia

Joint work with Sanja Rukavina

This work has been fully supported by Croatian Science Foundation under the project 6732

1. Boolean and generalized Boolean functions

2. Codes over $\mathbb{Z}_{2^k}$

3. Self-orthogonal $\mathbb{Z}_{2^k}$-codes constructed from Boolean functions

4. Self-orthogonal $\mathbb{Z}_{2^k}$-codes constructed from a pair of bent functions

Boolean and bent functions

Let $\mathbb{F}_2$ be the field of order 2.
A *Boolean function* on n variables is a mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2$.
The *Walsh-Hadamard transformation* of f is

$$W_f(v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \langle v, x \rangle}.$$

A *bent function* is a Boolean function f such that $W_f(v) = \pm 2^{\frac{n}{2}}$, for every $v \in \mathbb{F}_2^n$.

Generalized Boolean and gbent functions

Let $\mathbb{Z}_{2^k}$ be the ring of integers modulo 2^k.
A *generalized Boolean function* on n variables is a mapping $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$.
The *generalized Walsh-Hadamard transformation* of f is

$$\tilde{f}(v) = \sum_{x \in \mathbb{F}_2^n} \omega^{f(x)} (-1)^{\langle v,x \rangle},$$

where $\omega = e^{\frac{2\pi i}{2^k}}$.
A *gbent function* is a generalized Boolean function f such that $|\tilde{f}(v)| = 2^{\frac{n}{2}}$, for every $v \in \mathbb{F}_2^n$.

Theorem (K. U. Schmidt, 2009)

Let $n \geq 2$ be even, and let $a, b : \mathbb{F}_2^n \to \mathbb{F}_2$ be bent functions. Then $f : \mathbb{F}_2^{n+1} \to \mathbb{Z}_4$ given by

$$f(x, y) = 2a(x)(1 + y) + 2b(x)y + y, \; x \in \mathbb{F}_2^n, y \in \mathbb{F}_2,$$

is a gbent function.

$\mathbb{Z}_{2^k}$-codes

A $\mathbb{Z}_{2^k}$-*code* C of length n is an additive subgroup of $\mathbb{Z}_{2^k}^n$.
An element of C is called a *codeword* of C.
A code in which the circular shift of each codeword gives another codeword that belongs to the code is called a *cyclic code*.
A *generator matrix* of C is a matrix whose rows generate C.

Let C be a $\mathbb{Z}_{2^k}$-code of length n. The *dual code* $C^\perp$ of the code C is defined as

$$C^\perp = \{x \in \mathbb{Z}_{2^k}^n \mid \langle x, y\rangle = 0 \text{ for all } y \in C\},$$

where $\langle x, y\rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n \pmod{2^k}$ for $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$.

The code C is *self-orthogonal* if $C \subseteq C^\perp$.

Let $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_{2^k}^n$. The *Euclidean weight* of x is

$$wt_E(x) = \sum_{i=1}^{n} \min\{x_i^2, (2^k - x_i)^2\}.$$

Lemma (Bannai, Dougherty, Harada, Oura, 1999)

Let M be a generator matrix of a $\mathbb{Z}_{2^k}$-code C of length n. Suppose that the rows of M are codewords in $\mathbb{Z}_{2^k}^n$ with Euclidean weight a multiple of 2^{k+1} with any two rows orthogonal. Then C is a self-orthogonal code with all Euclidean weights a multiple of 2^{k+1}.

- O. S. Rothaus, On "Bent" Functions, *J. Comb. Theory Ser. A* **20** (1976), 300–305.

- C. Carlet, P. Gaborit, Hyper-bent functions and cyclic codes, *J. Comb. Theory Ser. A* **113**(3) (2006), 466–482.
- C. Tang, N. Li, Y. Qi, Z. Zhou, T. Helleseth, Linear Codes With Two or Three Weights From Weakly Regular Bent Functions, *IEEE Trans. Inform. Theory* **62**(3) (2016), 1166–1176.
- C. Ding, A. Munemasa, V. D. Tonchev, Bent Vectorial Functions, Codes and Designs, *IEEE Trans. Inform. Theory* **65**(11) (2019), 7533–7541.
- M. Shi, Y. Liu, H. Randriambololona, L. Sok, P. Solé, Trace codes over $\mathbb{Z}_4$, and Boolean functions, *Des. Codes Cryptogr.* **87** (2019), 1447–1455.

- A. K. Singh, N. Kumar, K. P. Shum, Cyclic self-orthogonal codes over finite chain ring, *Asian-Eur. J. Math.* **11**(6) (2018), 1850078.
- B. Kim, Construction for self-orthogonal codes over a certain non-chain Frobenius ring, *J. Korean Math. Soc.* **59**(1) (2022), 193-204.
- B. Kim, N. Han, Y. Lee, Self-orthogonal codes over $\mathbb{Z}_4$ arising from the chain ring $\mathbb{Z}_4[u]/\left\langle u^2+1\right\rangle$, *Finite Fields Appl.* **78** (2022), 101972.

- SB, S. RUKAVINA, Type IV-II codes over $\mathbb{Z}_4$ constructed from generalized bent functions, *Australas. J. Combin.* **84**(3) (2022), 341–356.
- SB, S. RUKAVINA, Construction of self-orthogonal $\mathbb{Z}_{2^k}$-codes, submitted, 2023.

An $n \times n$ *circulant matrix* is a matrix of the form

$$\begin{bmatrix} x_0 & x_{n-1} & \dots & x_2 & x_1 \\ x_1 & x_0 & x_{n-1} & \dots & x_2 \\ \vdots & & & & \vdots \\ x_{n-1} & \dots & \dots & x_1 & x_0 \end{bmatrix}.$$

- P. Stanica, T. Martinsen, S. Gangopadhyay, B. K. Singh, Bent and generalized bent Boolean functions, *Des. Codes Cryptogr.* **69** (2013), 77–94.

Theorem 1 (SB, S. Rukavina, 2023)

Let $a, b, c : \mathbb{F}_2^n \to \mathbb{F}_2$ be Boolean functions and let $3 \leq k \leq n$. Let $g_k^{(\epsilon)} : \mathbb{F}_2^{n+2} \to \mathbb{Z}_{2^k}$ be a generalized Boolean function given by

$$g_k^{(\epsilon)}(x, y, z) = 2^{k-1}a(x) + (2^{k-1}b(x) + 1)y + (2^{k-1}c(x) + 1)z + 2\epsilon yz,$$

$x \in \mathbb{F}_2^n, y, z \in \mathbb{F}_2$, where $\epsilon \in \{-1, 1\}$, and let $c_{g_k^{(\epsilon)}}$ be a codeword

$$(g_k^{(\epsilon)}((0, \ldots, 0)), g_k^{(\epsilon)}((0, \ldots, 0, 1)), \ldots, g_k^{(\epsilon)}((1, \ldots, 1))) \in \mathbb{Z}_{2^k}^{2^{n+2}}.$$

Let $C_{g_k^{(\epsilon)}}$ be a $\mathbb{Z}_{2^k}$-code generated by the $2^{n+2} \times 2^{n+2}$ circulant matrix whose first row is the codeword $c_{g_k^{(\epsilon)}}$. Then $C_{g_k^{(\epsilon)}}$ is a cyclic self-orthogonal $\mathbb{Z}_{2^k}$-code of length 2^{n+2}. If $b = c$, then all codewords in $C_{g_k^{(\epsilon)}}$ have Euclidean weights divisible by 2^{k+1}.

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) *design*, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks.
If the condition

$$|B_i \cap B_j| \equiv |B_k| \equiv 0 \pmod 2$$

is satisfied for all blocks B_i, B_j and B_k of $\mathcal{D}$, we say that $\mathcal{D}$ is a *self-orthogonal design*.

A k-dimensional subspace of $\mathbb{F}_2^n$ is called an $[n, k]$ *binary linear code*.
An element of a code is called a *codeword*.
The *support* of a codeword $x \in \mathbb{F}_2^n$ is the set of non-zero positions in x.
The *weight* of a codeword $x \in \mathbb{F}_2^n$ is the number of non-zero coordinates in x. If the minimum weight d of an $[n, k]$ binary linear code is known, then we refer to the code as an $[n, k, d]$ binary linear code.

The *binary residue code* of a $\mathbb{Z}_{2^k}$-code C is defined as

$$C^{(1)} = \{c \pmod 2 \,|\, c \in C\}.$$

The binary residue code of the $\mathbb{Z}_{2^k}$-code $C_{g_k^{(\epsilon)}}$, constructed as in Theorem 1, is a $[2^{n+2}, 3, 2^{n+1}]$ binary linear code. The supports of the minimum weight codewords in ${C_{g_k^{(\epsilon)}}}^{(1)}$ form a self-orthogonal 1-$(2^{n+2}, 2^{n+1}, 3)$ design with 6 blocks and block intersection numbers 0 and 2^n.

Example 1

Let $n = k = 3$,

$$a(x_1, x_2, x_3) = 1, \ b(x_1, x_2, x_3) = c(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2$$

and $\epsilon = -1$. Then

$$c_{g_3^{(-1)}} = 01540154411441140154411401544114 \in \mathbb{Z}_8^{32}$$

and $C_{g_3^{(-1)}}$ is a cyclic self-orthogonal $\mathbb{Z}_8$-code of length 32, where all codewords have Euclidean weights divisible by 16.

Proposition 1 (SB, S. Rukavina, 2022)

Let n be even, and let $a, b : \mathbb{F}_2^n \to \mathbb{F}_2$ be bent functions. Let $f : \mathbb{F}_2^{n+1} \to \mathbb{Z}_4$ be a gbent function given by $f(x, y) = 2a(x)(1 + y) + 2b(x)y + y,\ \ x \in \mathbb{F}_2^n,\ y \in \mathbb{F}_2$, and let c_f be a codeword

$$(f((0, \ldots, 0)), f((0, \ldots, 0, 1)), \ldots, f((1, \ldots, 1))) \in \mathbb{Z}_4^{2^{n+1}}.$$

Let C_f be a $\mathbb{Z}_4$-code generated by the $2^{n+1} \times 2^{n+1}$ circulant matrix whose first row is the codeword c_f. Then C_f is a cyclic self-orthogonal $\mathbb{Z}_4$-code of length 2^{n+1}, all its codewords have Euclidean weights divisible by 8.

Theorem 2 (SB, S. Rukavina, 2023)

Let n be even, and let $a, b : \mathbb{F}_2^n \to \mathbb{F}_2$ be bent functions. Let $k \geq 3$ and let $f_k^{(\epsilon)} : \mathbb{F}_2^{n+1} \to \mathbb{Z}_{2^k}$ be a generalized Boolean function given by

$$f_k^{(\epsilon)}(x, y) = 2^{k-1}a(x) + (2^{k-1}a(x) + 2^{k-1}b(x) + 2^{k-2}\epsilon)y,\ x \in \mathbb{F}_2^n, y \in \mathbb{F}_2,$$

where $\epsilon \in \{-1, 1\}$. Let $c_{f_k^{(\epsilon)}}$ be a codeword

$$(f_k^{(\epsilon)}((0, \ldots, 0)), f_k^{(\epsilon)}((0, \ldots, 0, 1)), \ldots, f_k^{(\epsilon)}((1, \ldots, 1))) \in \mathbb{Z}_{2^k}^{2^{n+1}}.$$

Let $C_{f_k^{(\epsilon)}}$ be a $\mathbb{Z}_{2^k}$-code generated by the $2^{n+1} \times 2^{n+1}$ circulant matrix whose first row is the codeword $c_{f_k^{(\epsilon)}}$. Then $C_{f_k^{(\epsilon)}}$ is a cyclic self-orthogonal $\mathbb{Z}_{2^k}$-code of length 2^{n+1} and all its codewords have Euclidean weights divisible by 2^{2k-1}.

Example 2

Let $n = 2,\ k = 3,$

$$a(x_1, x_2) = x_1x_2 + x_2,\ b(x_1, x_2) = x_1x_2 + x_1 + x_2$$

and $\epsilon = 1$. Then

$$c_{f_3^{(1)}} = 02460606 \in \mathbb{Z}_8^8$$

and $C_{f_3^{(1)}}$ is a cyclic self-orthogonal $\mathbb{Z}_8$-code of length 8, all its codewords have Euclidean weights divisible by 32.

Theorem 3 (SB, S. Rukavina, 2023)

Let n be even, and let $a, b : \mathbb{F}_2^n \to \mathbb{F}_2$ be bent functions. Let $k \geq 3$ and let $h_k^{(\epsilon)} : \mathbb{F}_2^{n+1} \to \mathbb{Z}_{2^k}$ be a generalized Boolean function given by

$$h_k^{(\epsilon)}(x, y) = 2^{k-1}a(x) + (2^{k-1}b(x) + 2^{k-2}\epsilon)y,\ x \in \mathbb{F}_2^n, y \in \mathbb{F}_2,$$

where $\epsilon \in \{-1, 1\}$, and let $c_{h_k^{(\epsilon)}}$ be a codeword

$$(h_k^{(\epsilon)}((0, \ldots, 0)), h_k^{(\epsilon)}((0, \ldots, 0, 1)), \ldots, h_k^{(\epsilon)}((1, \ldots, 1))) \in \mathbb{Z}_{2^k}^{2^{n+1}}.$$

Let $C_{h_k^{(\epsilon)}}$ be a $\mathbb{Z}_{2^k}$-code generated by the $2^{n+1} \times 2^{n+1}$ circulant matrix whose first row is the codeword $c_{h_k^{(\epsilon)}}$. Then $C_{h_k^{(\epsilon)}}$ is cyclic self-orthogonal $\mathbb{Z}_{2^k}$-code of length 2^{n+1} and all codewords in $C_{h_k^{(\epsilon)}}$ have Euclidean weights divisible by 2^{k+1}.

Example 3

Let $n = 2,\ k = 3,$

$$a(x_1, x_2) = x_1x_2 + x_2,\ b(x_1, x_2) = x_1x_2 + x_1 + x_2$$

and $\epsilon = 1$. Then

$$c_{h_3^{(1)}} = 02420606 \in \mathbb{Z}_8^8$$

and $C_{h_3^{(1)}}$ is a cyclic self-orthogonal $\mathbb{Z}_8$-code of length 8, all its codewords have Euclidean weights divisible by 16.

Thank you!