A construction of $\mathbb{Z}_4$-codes from generalized bent functions

Sara Ban

sban@math.uniri.hr

Department of Mathematics, University of Rijeka, Croatia

A joint work with Sanja Rukavina

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

1. Preliminaries

2. Codes constructed from gbent functions
   - Codes over $\mathbb{Z}_4$
   - Binary Type II self-dual codes

Let $\mathbb{F}_q$ be the field of order q, where q is a prime power. A code C over $\mathbb{F}_q$ of length n is any subset of $\mathbb{F}_q^n$.
A k-dimensional subspace of $\mathbb{F}_q^n$ is called an $[n, k]$ *q-ary linear code*.
An element of a code is called a *codeword*.
If $q = 2$, then the code is called *binary*.
The *weight* of a codeword $x \in \mathbb{F}_2^n$ is the number of non-zero coordinates in x.
Binary linear codes for which all codewords have weight divisible by four are called *doubly even*.

Let C be a binary linear code of length n. The *dual code* $C^{\perp}$ of C is defined as

$$C^{\perp} = \{x \in \mathbb{F}_2^n \mid \langle x, y \rangle = 0 \text{ for all } y \in C\},$$

where $\langle x, y \rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n \pmod 2$ for $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$.
The code C is *self-dual* if $C = C^{\perp}$.
A self-dual doubly even binary code is called a *Type II binary code*.

Let $\mathbb{Z}_4$ denote the ring of integers modulo 4. A linear code C of length n over $\mathbb{Z}_4$ (i.e., a $\mathbb{Z}_4$-*code*) is a $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^n$.
Two $\mathbb{Z}_4$-codes are *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates.
Denote the number of coordinates i (where $i = 0, 1, 2, 3$) in a codeword $x \in \mathbb{Z}_4^n$ by $n_i(x)$. The *Hamming weight* of a codeword x is $wt_H(x) = n_1(x) + n_2(x) + n_3(x)$, the *Lee weight* of x is $wt_L(x) = n_1(x) + 2n_2(x) + n_3(x)$ and the *Euclidean weight* of x is $wt_E(x) = n_1(x) + 4n_2(x) + n_3(x)$.

Let C be a $\mathbb{Z}_4$-code of length n. The *dual code* $C^\perp$ of the code C is defined as

$$C^\perp = \{x \in \mathbb{Z}_4^n \mid \langle x, y \rangle = 0 \text{ for all } y \in C\},$$

where $\langle x, y \rangle = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n \pmod 4$ for $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$.
The code C is *self-orthogonal* when $C \subseteq C^\perp$ and *self-dual* if $C = C^\perp$.

Type II $\mathbb{Z}_4$-codes are self-dual $\mathbb{Z}_4$-codes which have the property that all Euclidean weights are divisible by eight.
Type IV $\mathbb{Z}_4$-codes are self-dual $\mathbb{Z}_4$-codes with all codewords of even Hamming weight.
A Type IV code that is also Type II is called a *Type IV-II $\mathbb{Z}_4$-code*.

Every $\mathbb{Z}_4$-code C contains a set of $k_1 + k_2$ codewords $\{c_1, c_2, \ldots, c_{k_1}, c_{k_1+1}, \ldots, c_{k_1+k_2}\}$ such that every codeword in C is uniquely expressible in the form

$$\sum_{i=1}^{k_1} a_i c_i + \sum_{i=k_1+1}^{k_1+k_2} a_i c_i,$$

where $a_i \in \mathbb{Z}_4$ and c_i has at least one coordinate equal to 1 or 3, for $1 \leq i \leq k_1$, $a_i \in \mathbb{Z}_2$ and c_i has all coordinates equal to 0 or 2, for $k_1 + 1 \leq i \leq k_1 + k_2$.
We say that C is of *type* $4^{k_1} 2^{k_2}$.
The matrix whose rows are c_i, $1 \leq i \leq k_1 + k_2$, is called a *generator matrix* for C.

A generator matrix G of a $\mathbb{Z}_4$-code C is in *standard form* if

$$G = \begin{bmatrix} I_{k_1} & A & B_1 + 2B_2 \\ O & 2I_{k_2} & 2D \end{bmatrix},$$

where A, B_1, B_2 and D are matrices with entries from $\mathbb{Z}_2$, O is the $k_2 \times k_1$ null matrix, and I_m denotes the identity matrix of order m.

Let C be a $\mathbb{Z}_4$-code of length n. There are two binary linear codes of length n associated with C: the binary code

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

which is called the *residue code* of C, and the binary code

$$C^{(2)} = \{c \in \mathbb{Z}_2^n \mid 2c \in C\},$$

which is called the *torsion code* of C.

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 $v \in \mathbb{F}_2^n$.

A *generalized Boolean function* on n variables is a mapping $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^h}$.
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 $\omega = e^{\frac{2\pi i}{2^h}}$.
A *generalized bent function (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 $m \geq 3$ be odd, and let $a, b : \mathbb{F}_2^{m-1} \to \mathbb{F}_2$ be bent functions. Then $f : \mathbb{F}_2^m \to \mathbb{Z}_4$ given by

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

is a gbent function.

Theorem 1 (SB, S. Rukavina, 2021)

Let $m \geq 3$ be odd, and let $a, b : \mathbb{F}_2^{m-1} \to \mathbb{F}_2$ be bent functions. Let $f : \mathbb{F}_2^m \to \mathbb{Z}_4$ be a gbent function given by

$$f(x, y) = 2a(x)(1 + y) + 2b(x)y + y,$$

$x \in \mathbb{F}_2^{m-1}$, $y \in \mathbb{F}_2$, and let c_f be a codeword

$$(f((0, \dots, 0)), f((0, \dots, 0, 1)), \dots, f((1, \dots, 1))) \in \mathbb{Z}_4^{2^m}.$$

Let C_f be a $\mathbb{Z}_4$-code generated by the $2^m \times 2^m$ circulant matrix whose first row is the codeword c_f. Then C_f is a self-orthogonal $\mathbb{Z}_4$-code of length 2^m and all its codewords have Euclidean weights divisible by 8. The residue code of C_f has dimension 2.

Theorem 2 (SB, S. Rukavina, 2021)

Let C_f be a $\mathbb{Z}_4$-code of type $4^2 2^{k_2}$ constructed as in Theorem 1. Let G be a generator matrix of C_f in standard form. Let $k_3 = 2^m - 2^2 - k_2$ and let

$$\widetilde{D} = \left[\begin{array}{ccc} O & 2I_{k_3} & H \end{array} \right]$$

be a $k_3 \times 2^m$ matrix, where O is the $k_3 \times (k_2 + 2)$ null matrix and H is a $k_3 \times 2$ matrix whose rows $h_i, 1 \le i \le k_3$ are defined as follows.
If k_2 is odd, then

$$h_i = \begin{cases} (0,2), & \text{if } i \text{ is odd} \\ (2,0), & \text{if } i \text{ is even} \end{cases} .$$

If k_2 is even, then

$$h_i = \begin{cases} (2,0), & \text{if } i \text{ is odd} \\ (0,2), & \text{if } i \text{ is even} \end{cases} .$$

(i) The code $\widetilde{C_f}$ generated by the matrix $\widetilde{G} = \begin{bmatrix} G \\ \widetilde{D} \end{bmatrix}$ is a Type II $\mathbb{Z}_4$-code of length 2^m.

(ii) If $m \geq 5$, then $\widetilde{C_f}$ is a Type IV $\mathbb{Z}_4$-code.

(iii) Up to equivalence, $\widetilde{C_f}$ does not depend on the choice of bent functions a and b.

Theorem 3 (SB, S. Rukavina, 2021)

Let $\widetilde{C_f}$ be a Type II $\mathbb{Z}_4$-code of length 2^m for odd $m, m \geq 3$, constructed as in Theorem 2, and let $(A'_0, \ldots, A'_{2^m})$ be the weight distribution of its torsion code $\widetilde{C_f}^{(2)}$. Then:

(i) $\widetilde{C_f}$ has Euclidean weight distribution $(W_0^E, \ldots, W_{2^{m+2}}^E)$ with $W_i^E = 0$ for $i \not\equiv 0$ $(mod\ 8)$ and, for i divisible by 8, it holds

$$W_i^E = A'_{\frac{i}{4}} + s_i + t_i,$$

(ii) if $m \geq 5$, then $\widetilde{C_f}$ has Lee weight distribution $(W_0^L, \ldots, W_{2^{m+1}}^L)$ with $W_i^L = 0$ for $i \not\equiv 0$ $(mod\ 4)$ and, for i divisible by 4, it holds

$$W_i^L = A'_{\frac{i}{2}} + s_i + u_i,$$

where

$$A'_j = \frac{1}{2}\left(\binom{2^m}{j} + \sum_{l=0}^{j}(-1)^l \binom{2^{m-1}}{l}\binom{2^{m-1}}{j-l}\right)$$

for even j and $A'_j = 0$ for odd j, $j = 0, \ldots, 2^m$, and

$$s_i = \begin{cases} 2^{2^m-2}, & \text{if } i = 2^m \\ 0, & \text{otherwise} \end{cases},$$

$$t_i = \begin{cases} 2^{2^{m-1}}\binom{2^{m-1}}{(2i-2^m)/8}, & \text{if } 2^{m-1} \le i \le 5 \cdot 2^{m-1} \\ 0, & \text{otherwise} \end{cases},$$

$$u_i = \begin{cases} 2^{2^{m-1}}\binom{2^{m-1}}{(2i-2^m)/4}, & \text{if } 2^{m-1} \le i \le 3 \cdot 2^{m-1} \\ 0, & \text{otherwise} \end{cases}.$$

The *Gray map* $\phi : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$ is the componentwise extension of the map $\psi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ defined by

$$\psi(0) = (0,0),\ \psi(1) = (0,1),\ \psi(2) = (1,1),\ \psi(3) = (1,0).$$

Theorem (S. T. Dougherty, P. Gaborit, M. Harada, A. Munemasa, P. Solé, 1999)

If C is a Type IV $\mathbb{Z}_4$-code, then its Gray image is a Type II binary code.

Corollary (SB, S. Rukavina 2021)

Let $\widetilde{C_f}$ be a Type II $\mathbb{Z}_4$-code of length 2^m for odd $m, m \geq 3$, constructed as in Theorem 2. Then $\phi(\widetilde{C_f})$ is a self-dual binary code of length 2^{m+1}. If $m \geq 5$, then $\phi(\widetilde{C_f})$ is doubly even.

- $(a, b) = (x_1x_2, x_1 + x_1x_2)$

$C_f \Longrightarrow$ 1-$(8, 5, 5)$ design with 8 blocks and block intersection numbers 2 and 4 $\Longrightarrow$ the block intersection graph G_2 is a SRG with parameters $(8, 4, 0, 4)$
$C_f^\perp \Longrightarrow$ 1-$(8, 4, 2)$ design with 4 blocks and block intersection numbers 0 and 2 (an affine resolvable 1-design)

- $(a, b) = (x_1x_2 + x_1x_3 + x_2x_4, x_1x_2 + x_3x_4)$

$C_f^\perp \Longrightarrow$ 1-$(32, 8, 7)$ with 28 blocks and block intersection numbers 0 and 4 (an affine resolvable 1-design) $\Longrightarrow$ the block intersection graph G_0 is a SRG with parameters $(28, 15, 6, 10)$

Thank you!