Construction of extremal Type II $\mathbb{Z}_8$-codes

Sara Ban Martinović

sban@math.uniri.hr

Faculty of Mathematics, University of Rijeka

Joint work with Sanja Rukavina

This work was supported by the Croatian Science Foundation under the project number HRZZ–IP–2022–10–4571 and by the University of Rijeka under the project uniri-iskusni-prirod-23-62

Croatian Science Foundation

1. Type II $\mathbb{Z}_{2k}$-codes
2. Doubling method
3. Construction of extremal Type II $\mathbb{Z}_8$-codes

S. Ban, S. Rukavina, *Construction of extremal Type II $\mathbb{Z}_8$-codes via doubling method*, arXiv: 2405.00584 (2024).

Let $\mathbb{Z}_{2k}$ denote the ring of integers modulo $2k$. A linear code C of length n over $\mathbb{Z}_{2k}$ (i.e., a $\mathbb{Z}_{2k}$-*code*) is a $\mathbb{Z}_{2k}$-submodule of $\mathbb{Z}_{2k}^n$.

Two $\mathbb{Z}_{2k}$-codes are *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates.

An element of a code is called a *codeword*.

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

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

We will denote by $d_E(C)$ the minimum Euclidean weight of the code C.

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

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

where $\langle x, y \rangle = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n \pmod{2k}$ 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 $C = C^{\perp}$.

Type II $\mathbb{Z}_{2k}$*-codes* are self-dual $\mathbb{Z}_{2k}$-codes which have the property that all Euclidean weights are divisible by $4k$.

E. Bannai, S. T. Dougherty, M. Harada, M. Oura, *Type II Codes, Even Unimodular Lattices and Invariant Rings*, IEEE Trans. Inf. Theory, **45**(4), 1194–1205 (1999).

Theorem

Let C be a Type II $\mathbb{Z}_{2k}$-code of length n. Then $n \equiv 0 \pmod 8$ and

$$d_E(C) \leq 4k \left\lfloor \frac{n}{24} \right\rfloor + 4k \tag{1}$$

holds for $k \leq 6$, and for $k \geq 7$ it holds under the assumption that $\left\lfloor \frac{n}{24} \right\rfloor \leq k - 2$.

We say that a Type II $\mathbb{Z}_{2k}$-code meeting (1) with equality is *extremal*.

Extremal Type II $\mathbb{Z}_8$-codes of length up to 48 can be found in:

E. Bannai, S. T. Dougherty, M. Harada, M. Oura, *Type II Codes, Even Unimodular Lattices and Invariant Rings*, IEEE Trans. Inf. Theory, **45**(4), 1194–1205 (1999).

R. Chapman, P. Solé, *Universal codes and unimodular lattices*, J. de th. des nombres de Bordeaux, **8**, 369–376 (1996).

J. H. Conway, N. J. A. Sloane, *Sphere Packing, Lattices and Groups (3rd ed.)*, Springer-Verlag, New York (1999).

S. Georgiou, M. Harada, C. Koukouvinos, *Orthogonal designs and Type II codes over $\mathbb{Z}_{2k}$*, Des. Codes Cryptogr. **25**, 163–174 (2002).

T. A. Gulliver, M. Harada, *Extremal Self-Dual Codes over $\mathbb{Z}_6, \mathbb{Z}_8$ and $\mathbb{Z}_{10}$*, AKCE J. Graphs. Combin. **2**(1), 11–24 (2005).

A *generator matrix* of a $\mathbb{Z}_{2k}$-code C is a matrix whose rows generate C.

Each code C over $\mathbb{Z}_{2^m}$ is permutation-equivalent to a code with a generator matrix in *standard form*

$$\begin{pmatrix} I_{k_1} & A_{1,2} & A_{1,3} & A_{1,4} & \cdots & \cdots & A_{1,m+1} \\ 0 & 2I_{k_2} & 2A_{2,3} & 2A_{2,4} & \cdots & \cdots & 2A_{2,m+1} \\ 0 & 0 & 4I_{k_3} & 4A_{3,4} & \cdots & \cdots & 4A_{3,m+1} \\ \vdots & \vdots & \vdots & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 2^{m-1}I_{k_m} & 2^{m-1}A_{m,m+1} \end{pmatrix},$$

where the matrix $A_{i,j}$ has elements in $\mathbb{Z}_{2^{j-1}}$.
We say that C is of *type* $(k_1, k_2, k_3, \ldots, k_m)$.

If C is a $\mathbb{Z}_{2^m}$-code, then the code

$$C^{(2^k)} = \{x \pmod{2^k} \,|\, x \in C\},\ 1 \leq k \leq m-1,$$

is the $\mathbb{Z}_{2^k}$-*residue code* of C.

Doubling method

Theorem (SBM, S. Rukavina, 202*)

Let $k \geq 2$. Let C be a Type II $\mathbb{Z}_{2k}$-code of length n and let $n_i(x)$ denote the number of coordinates i in $x \in \mathbb{Z}_{2k}^n$. Let $ku \in \mathbb{Z}_{2k}^n \setminus C$ be a codeword with all coordinates equal to 0 or k with the following property: if k is odd, $n_k(ku)$ is divisible by four, if k is even and not divisible by four, $n_k(ku)$ is even. Let $C_0 = \{v \in C \mid \langle ku, v \rangle = 0\}$. Then $\widetilde{C} = C_0 \oplus \langle ku \rangle$ is a Type II $\mathbb{Z}_{2k}$-code.

Theorem (SBM, S. Rukavina, 202*)

Let $m \geq 2$. Let C be a Type II $\mathbb{Z}_{2^m}$-code of length n and type $(k_1, k_2, \ldots, k_m)$. The choice of $2^{m-1}u \in \mathbb{Z}_{2^m}^n \setminus C$ in previous theorem can be limited to codewords with zeroes on the first $k_1 + k_2 + \cdots + k_m$ coordinates.

Theorem (SBM, S. Rukavina, 202*)

Let $m \geq 2$. Let C be a Type II $\mathbb{Z}_{2^m}$-code of length n and type $(k_1, k_2, \ldots, k_m)$. Let G be a generator matrix of C in standard form and G_i the i^{th} row of G. Let $2^{m-1}u \in \mathbb{Z}_{2^m}^n \setminus C$ be a codeword with zeroes on the first $k_1 + k_2 + \cdots + k_m$ coordinate positions such that $n_{2^{m-1}}(2^{m-1}u)$ is even if $m = 2$. Let $B = \{G_1, \ldots, G_{k_1+k_2+\cdots+k_m}\}$. The following process yields a generator matrix $\widetilde{G}$ of the $\mathbb{Z}_{2^m}$-code $\widetilde{C}$ obtained from C and $2^{m-1}u$ by the doubling method.

Step 1: Let $B_E = \{G_i \in B \mid \langle G_i, 2^{m-1}u \rangle = 0\}$ and $B_O = B \setminus B_E$.

Step 2: Pick $G_i \in B_O$ arbitrarily. Define $B_O' = \{G_i + G_j \mid G_j \in B_O\}$.

Step 3: Let $\widetilde{G}$ be a matrix whose rows are the elements of the set $B_O' \cup B_E \cup \{2^{m-1}u\}$.

The resultant code $\widetilde{C}$ is of type

$$\begin{cases} (k_1 - 1, k_2 + 2), & \text{if } m = 2, \\ (k_1 - 1, k_2 + 1, k_3 + 1), & \text{if } m = 3, \\ (k_1 - 1, k_2 + 1, k_3, \ldots, k_{m-1}, k_m + 1), & \text{if } m \geq 4. \end{cases}$$

The code $\widetilde{C}$ is independent of the choice of G_i in Step 2.

Construction of extremal Type II $\mathbb{Z}_8$-codes

Theorem (SBM, S. Rukavina, 202*)

Let $n \in \{24, 32, 40\}$. Denote by $S_i(w)$ the set of positions with the element $i \in \mathbb{Z}_8$ in $w \in \mathbb{Z}_8^n$. Let C be an extremal Type II $\mathbb{Z}_8$-code of length n and type (k_1, k_2, k_3) where $C^{(4)}$ is extremal. Suppose $4u \in \mathbb{Z}_8^n$ is a codeword with all coordinates equal to 0 or 4 such that $S_4(4u) \subseteq \{k_1 + k_2 + k_3 + 1, \ldots, n\}$, where $|S_4(4u)| \geq 2$. If there is no codeword v of C that satisfies any of the following conditions:

1. $S_3(v) \cup S_4(v) \cup S_5(v) \subseteq S_4(4u) \subseteq S_2(v) \cup S_3(v) \cup S_4(v) \cup S_5(v) \cup S_6(v)$ and
$$wt_E(v \pmod 4) = 16,$$
2. $|S_4(4u) \setminus S_4(v)| + |S_4(v) \setminus S_4(4u)| = 1$ and $wt_E(v \pmod 4) = 0$,

then the Type II $\mathbb{Z}_8$-code $\widetilde{C}$ generated by $4u$ and C using the doubling method is extremal. These choices of $4u$ are the only candidates for the code C in the doubling method which lead to an extremal code.

Algorithm C

Let $n \in \{24, 32, 40\}$. Denote by $S_i(w)$ the set of positions with the element $i \in \mathbb{Z}_8$ in $w \in \mathbb{Z}_8^n$. Let C be an extremal Type II $\mathbb{Z}_8$-code of length n and type $(\frac{n}{2}, 0, 0)$, where $C^{(4)}$ is extremal, with the generator matrix $G = \begin{bmatrix} I_{\frac{n}{2}} & A \end{bmatrix}$ in the standard form.

1. Let $v = (v_1, \ldots, v_n) \in C^{(4)}$ be a codeword of Euclidean weight 16.

1.2. Let $F_v = \{v_1, \ldots, v_{\frac{n}{2}}\}$, $A_v = S_2(v) \cap F_v$ and $B_v = S_3(v) \cap F_v$.

1.3. Repeat the following steps on all $A \subseteq A_v$:

1.3.1. Calculate $v' = \sum_{i=1}^{\frac{n}{2}} v_i G_i + 4s_A + 4s_{B_v}$, where s_A is the sum of rows in the generator matrix G of C with row indices in A and s_{B_v} is the sum of rows in G with row indices in B_v.

1.3.2. Let

$$O_{v'} = (S_2(v') \cup S_6(v')) \cap \left\{\frac{n}{2} + 1, \ldots, n\right\},$$

$$P_{v'} = S_4(v') \cap \left\{\frac{n}{2} + 1, \ldots, n\right\},$$

$$Q_{v'} = (S_3(v') \cup S_5(v')) \cap \left\{\frac{n}{2} + 1, \ldots, n\right\}.$$

1.3.3. Let $\mathcal{B}$ be the collection of all sets

$$B = O \cup P_{v'} \cup Q_{v'}, \; O \subseteq O_{v'},$$

where $|B| \geq 2$.

2. For all $i \in \{1, \ldots, \frac{n}{2}\}$, do the following.

2.1. Let $O_i = S_4(4G_i) \cap \left\{\frac{n}{2} + 1, \ldots, n\right\}$, where G_i is the i^{th} row of G.

2.2. Include all O_i such that $|O_i| \geq 2$ in $\mathcal{B}$.

Theorem (SBM, S. Rukavina, 202*)

Let $n \in \{24, 32, 40\}$. Denote by $S_i(w)$ the set of positions with the element $i \in \mathbb{Z}_8$ in $w \in \mathbb{Z}_8^n$. Let C be an extremal Type II $\mathbb{Z}_8$-code of length n and type $(\frac{n}{2}, 0, 0)$, where $C^{(4)}$ is extremal. Furthermore, let $\mathcal{S}$ be the collection of all $S \subseteq \left\{\frac{n}{2}+1, \ldots, n\right\}$ such that $|S| \geq 2$. Then $\mathcal{G} = \mathcal{S} \setminus \mathcal{B}$ is the set of all possible $S_4(4u)$ for the code C in the doubling method which lead to an extremal Type II $\mathbb{Z}_8$-code $\widetilde{C}$ of length n and type $(\frac{n}{2}-1, 1, 1)$, where $\mathcal{B}$ is the set obtained by applying Algorithm C.

Six inequivalent extremal Type II $\mathbb{Z}_8$-codes of length 32 are known: $C_{8,32,i},\ i = 1, \ldots, 5$ from

M. Harada, *Construction of extremal Type II $\mathbb{Z}_{2k}$-codes*, Finite Fields Appl. **87**, 102154 (2023).

and D_{32} from

T. A. Gulliver, M. Harada, *Extremal Self-Dual Codes over $\mathbb{Z}_6, \mathbb{Z}_8$ and $\mathbb{Z}_{10}$*, AKCE J. Graphs. Combin. **2**(1), 11–24 (2005).

Since all of them are of type $(16, 0, 0)$, we investigated the possibility of constructing new extremal Type II $\mathbb{Z}_8$-codes of length 32 by using the introduced doubling method.

Codes $C_{8,32,1}$ and $C_{8,32,2}$ have extremal $\mathbb{Z}_4$-residue codes. We applied Algorithm C and found 23067 candidates $4u$ for a construction of extremal Type II $\mathbb{Z}_8$-codes of type $(15, 1, 1)$ and length 32 from $C_{8,32,1}$ by doubling method. Also, we found 22818 candidates $4u$ for a construction of extremal Type II $\mathbb{Z}_8$-codes of type $(15, 1, 1)$ and length 32 from $C_{8,32,2}$ by doubling method.

Further, D_{32} has an extremal $\mathbb{Z}_4$-residue code. We applied Algorithm C and found 22965 candidates $4u$ for a construction of extremal Type II $\mathbb{Z}_8$-codes of type $(15, 1, 1)$ and length 32 from D_{32} by doubling method.

Using Magma, we calculated the weight distributions of the corresponding 68850 binary residue codes and obtained that all constructed extremal Type II $\mathbb{Z}_8$-codes are distributed into 10 classes:

	i	0	8	12	16	20	24	32
${C_1}^{(2)}$	W_i	1	316	6912	18310	6912	316	1
${C_2}^{(2)}$	W_i	1	332	6848	18406	6848	332	1
${C_3}^{(2)}$	W_i	1	337	6888	18259	7000	283	0
${C_4}^{(2)}$	W_i	1	305	6952	18259	6936	315	0
${C_5}^{(2)}$	W_i	1	308	6944	18262	6944	308	1
${C_6}^{(2)}$	W_i	1	300	6976	18214	6976	300	1
${C_7}^{(2)}$	W_i	1	364	6720	18598	6720	364	1
${C_8}^{(2)}$	W_i	1	380	7168	17670	7168	380	1
${C_9}^{(2)}$	W_i	1	324	6880	18358	6880	324	1
${C_{10}}^{(2)}$	W_i	1	340	6816	18454	6816	340	1

For each of the obtained weight distribution classes we give the generator matrix in standard form for the following class representatives:

$$C_1 = C_{8,32,1_0} \oplus \langle 4u \rangle \,, \; S_4(4u) = \{17, 19, 21, 22\},$$

$$C_2 = C_{8,32,1_0} \oplus \langle 4u \rangle \,, \; S_4(4u) = \{17, 18, 20, 21\},$$

$$C_3 = C_{8,32,1_0} \oplus \langle 4u \rangle \,, \; S_4(4u) = \{17, 19, 21\},$$

$$C_4 = C_{8,32,1_0} \oplus \langle 4u \rangle \,, \; S_4(4u) = \{17, 19, 20, 21, 22\},$$

$$C_5 = C_{8,32,1_0} \oplus \langle 4u \rangle \,, \; S_4(4u) = \{17, 18, 19, 20\},$$

$$C_6 = C_{8,32,1_0} \oplus \langle 4u \rangle \,, \; S_4(4u) = \{17, 18, 19, 20, 21, 22\},$$

$$C_7 = C_{8,32,1_0} \oplus \langle 4u \rangle \,, \; S_4(4u) = \{18, 24, 25, 27\},$$

$$C_8 = C_{8,32,1_0} \oplus \langle 4u \rangle \,, \; S_4(4u) = \{20, 25\},$$

$$C_9 = C_{8,32,2_0} \oplus \langle 4u \rangle \,, \; S_4(4u) = \{17, 18, 19, 21\},$$

$$C_{10} = C_{8,32,2_0} \oplus \langle 4u \rangle \,, \; S_4(4u) = \{17, 21, 24, 25\}.$$

Those are, respectively:

$$G_1 = \begin{pmatrix} 10000000000000003476716356020474 \\ 01000000000000001703275645602047 \\ 00100000000000002574363514560204 \\ 00010000000000010615011726731415 \\ 00001000000000001365303604145602 \\ 00000100000000013130517745777155 \\ 00000010000000012611632063324043 \\ 00000001000000011163700305167532 \\ 00000000100000003474020675235254 \\ 00000000010000002347402047523525 \\ 00000000001000000234740234752352 \\ 00000000000100013461057440750622 \\ 00000000000010011200362013622110 \\ 00000000000001011426617330117347 \\ 00000000000000100100242336536347 \\ 00000000000000022004046042646062 \\ 00000000000000004040440000000000 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 10000000000000003032756356020474 \\ 01000000000000011003437173330306 \\ 00100000000000002574363514560204 \\ 00010000000000003257436341456020 \\ 00001000000000001721343604145602 \\ 00000100000000002532574360414560 \\ 00000010000000001657657406041456 \\ 00000001000000010665127256332404 \\ 00000000100000013130222123763513 \\ 00000000010000002347402047523525 \\ 00000000001000010770142562400611 \\ 00000000000100012163276311123574 \\ 00000000000010010346541764075062 \\ 00000000000001000464634753634752 \\ 00000000000000111142225713011734 \\ 00000000000000020200404664264606 \\ 00000000000000004404400000000000 \end{pmatrix},$$

$$
G_3 = \begin{pmatrix}
10000000000000010034371733303061 \\
01000000000000012301250222165434 \\
00100000000000002574363514560204 \\
00010000000000003257436341456020 \\
00001000000000001365343604145602 \\
00000100000000002532574360414560 \\
00000010000000001213657406041456 \\
00000001000000011163740305167532 \\
00000000100000003474020675235254 \\
00000000010000002347402047523525 \\
00000000001000000234740234752352 \\
00000000000100002063074063475235 \\
00000000000010011200362013622110 \\
00000000000001000020634753634752 \\
00000000000000100100202336536347 \\
00000000000000022004046042646062 \\
00000000000000004040400000000000
\end{pmatrix}, \quad
G_4 = \begin{pmatrix}
10000000000000003472716356020474 \\
01000000000000012305210222165434 \\
00100000000000002574363514560204 \\
00010000000000003257436341456020 \\
00001000000000012767326261420277 \\
00000100000000013130517745777155 \\
00000010000000001217617406041456 \\
00000001000000000561765720604145 \\
00000000100000003474020675235254 \\
00000000010000013745425424006112 \\
00000000001000000234740234752352 \\
00000000000100002067034063475235 \\
00000000000010011200362013622110 \\
00000000000001011422617330117347 \\
00000000000000100104242336536347 \\
00000000000000022004046042646062 \\
00000000000000004044400000000000
\end{pmatrix},
$$

$$G_5 = \begin{pmatrix} 10000000000000003072356356020474 \\ 01000000000000011003437173330306 \\ 00100000000000002574363514560204 \\ 00010000000000013753230677104367 \\ 00001000000000011465545132673141 \\ 00000100000000002532574360414560 \\ 00000010000000011313051734577715 \\ 00000001000000000161325720604145 \\ 00000000100000003474020675235254 \\ 00000000010000002347402047523525 \\ 00000000001000010730542562400611 \\ 00000000000100012163276311123574 \\ 00000000000010000602347436347523 \\ 00000000000001000424234753634752 \\ 00000000000000111102625713011734 \\ 00000000000000020200404664264606 \\ 00000000000000004444000000000000 \end{pmatrix}, \quad G_6 = \begin{pmatrix} 10000000000000003072716356020474 \\ 01000000000000001307275645602047 \\ 00100000000000001227052504221654 3 \\ 00010000000000003257436341456020 \\ 00001000000000001761303604145602 \\ 00000100000000002532574360414560 \\ 00000010000000001617617406041456 \\ 00000001000000010665127256332404 \\ 00000000100000003474020675235254 \\ 00000000010000002347402047523525 \\ 00000000001000000234740234752352 \\ 00000000000100002467034063475235 \\ 00000000000010010306501764075062 \\ 00000000000001010120036201362211 \\ 00000000000000111102265713011734 \\ 00000000000000020200404664264606 \\ 00000000000000004444440000000000 \end{pmatrix},$$

$$
G_7 = \begin{pmatrix}
10000000000000000736356436520474 \\
01000000000000011641650322265434 \\
00100000000000001274363114560204 \\
00010000000000013455451236631415 \\
00001000000000001525743364045602 \\
00000100000000000232574170214560 \\
00000010000000000553257246041456 \\
00000001000000002425325130604145 \\
00000000100000011472043462110641 \\
00000000010000001247402747023525 \\
00000000001000003034740664752352 \\
00000000000100000623474443275235 \\
00000000000010003002347646347523 \\
00000000000001002460234433134752 \\
00000000000000101440602576736347 \\
00000000000000022204046442046062 \\
00000000000000004000000440400000
\end{pmatrix}, \quad
G_8 = \begin{pmatrix}
10000000000000010576150634556733 \\
01000000000000013007437113330306 \\
00100000000000010630165062216543 \\
00010000000000013313230677104367 \\
00001000000000013465545112673141 \\
00000100000000002536574320414560 \\
00000010000000013313051714577715 \\
00000001000000011661127206332404 \\
00000000100000012534622173763513 \\
00000000010000013403204365251064 \\
00000000001000012370542542400611 \\
00000000000100011163276321123574 \\
00000000000010012746141744075062 \\
00000000000001010120036201362211 \\
00000000000000102402023415363475 \\
00000000000000022204404604264606 \\
00000000000000004004000000000000
\end{pmatrix},
$$

$$G_9 = \begin{pmatrix} 10000000000000003076052565220712 \\ 01000000000000003743645266522071 \\ 00100000000000010566173551245033 \\ 00010000000000003637436417665220 \\ 00001000000000000723343601766522 \\ 00000100000000002436374360176652 \\ 00000010000000013075046441402411 \\ 00000001000000000164763736601766 \\ 00000000100000010041231556227000 \\ 00000000010000003221702247363425 \\ 00000000001000002762570234736342 \\ 00000000000100002350263252546347 \\ 00000000000010000663221746347363 \\ 00000000000001001066322154634736 \\ 00000000000000103546232225463473 \\ 00000000000000020024026046066460 \\ 00000000000000004440400000000000 \end{pmatrix}, \quad G_{10} = \begin{pmatrix} 10000000000000003436052125220712 \\ 01000000000000011653420430260330 \\ 00100000000000010204547300310546 \\ 00010000000000003637436417665220 \\ 00001000000000012273526053424061 \\ 00000100000000002436374360176652 \\ 00000010000000013153412630555124 \\ 00000001000000012434146100347225 \\ 00000000100000002217022573634254 \\ 00000000010000003221702247363425 \\ 00000000001000002322570674736342 \\ 00000000000100002632617423473634 \\ 00000000000010012573404550005622 \\ 00000000000001001066322154634736 \\ 00000000000000111016015037121732 \\ 00000000000000020620046064204606 \\ 00000000000000004000400440000000 \end{pmatrix}.$$

According to

M. Grassl, *Code Tables: Bounds on the parameters of various types of codes:*

`http://www.codetables.de/`,

binary $[32, 15, 8]$ codes are the optimal binary $[32, 15]$ codes.
Therefore, all constructed extremal Type II $\mathbb{Z}_8$-codes of length 32 have optimal binary residue codes.

Theorem (SBM, S. Rukavina, 202*)

There are at least 16 inequivalent extremal Type II $\mathbb{Z}_8$-codes of length 32.