AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **42** (2008), Pages 177–188

Self-dual $\boldsymbol{Z}_4$-codes of Type IV generated by skew-Hadamard matrices and conference matrices

Mieko Yamada

Division of Mathematical and Physical Sciences
Graduate School of Natural Science and Technology
Kanazawa University
Japan
myamada@kenroku.kanazawa-u.ac.jp

Abstract

In this paper, we give families of self-dual $\boldsymbol{Z}_4$-codes of Type IV-I and Type IV-II generated by conference matrices and skew-Hadamard matrices. Furthermore, we give a family of self-dual $\boldsymbol{Z}_4$-codes of Type IV-I generated by bordered skew-Hadamard matrices.

1 Introduction

In 1994, Hammons et al. showed that certain binary nonlinear codes are the binary image of linear codes over the Galois ring $\mathrm{GR}(4, m)$, an extension ring of $\boldsymbol{Z}_4 = \boldsymbol{Z}/4\boldsymbol{Z}$ [7]. Active research on $\boldsymbol{Z}_4$-codes has been undertaken since their paper was published.

The distinct rows of an Hadamard matrix are orthogonal. If we recognize the entries 1 and -1 of an Hadamard matrix H_{4n} of order $4n$ as the elements of $\boldsymbol{Z}_4$, then the $\boldsymbol{Z}_4$-code generated by H_{4n} is self-orthogonal. In 1999, Charnes proved that if H_1 and H_2 are H-equivalent, then the $\boldsymbol{Z}_4$-codes generated by H_1 and H_2 are equivalent [3]. Solé showed that if an Hadamard matrix H_{4n} has order $4n$ and n is odd, then the $\boldsymbol{Z}_4$-code generated by H_{4n} is self-dual and equivalent to Klemm's code [3]. Charnes and Seberry considered the $\boldsymbol{Z}_4$-code generated by a weighing matrix $W(n, 4)$. They proved that if n is even, then it is a tetrad code and if it has type $4^{(n-4)/2}2^4$, then it is a self-dual code [4].

Self-dual $\boldsymbol{Z}_4$-codes of lengths up to 20 are classified [2, 5, 6, 8, 9]. A Type II $\boldsymbol{Z}_4$-code is a self-dual code which has the property that all Euclidean weights are divisible by 8. A self-dual $\boldsymbol{Z}_4$-code which is not a Type II code is called a Type I $\boldsymbol{Z}_4$-code. A Type IV $\boldsymbol{Z}_4$-code is a self-dual code with all codewords of even Hamming weight. A type IV code which is also Type I or Type II, is called a TypeIV-I, or a Type IV-II code respectively. Two infinite families of Type IV codes are known, that is, Klemm's codes and $C_{m,r}$ codes [1, 5].

In this paper, we give families of self-dual $\boldsymbol{Z}_4$-codes of Type IV-I and Type IV-II generated by conference matrices and skew-Hadamard matrices. Furthermore we give a family of self-dual $\boldsymbol{Z}_4$-codes of Type IV-I generated by bordered skew-Hadamard matrices.

2 Self-dual $\boldsymbol{Z}_4$-codes

An additive subgroup of $\boldsymbol{Z}_4^n$ is called a $\boldsymbol{Z}_4$-code of length n. We define an inner product on $\boldsymbol{Z}_4^n$ by $\boldsymbol{a} \cdot \boldsymbol{b} = \sum_{i=1}^n a_i \cdot b_i$ for vectors $\boldsymbol{a} = (a_1, a_2, \cdots, a_n)$ and $\boldsymbol{b} = (b_1, b_2, \cdots, b_n)$. The dual code $C^\perp$ of a $\boldsymbol{Z}_4$-code C is defined as $C^\perp = \{\boldsymbol{x} \in \boldsymbol{Z}_4^n \,|\boldsymbol{x} \cdot \boldsymbol{y} = 0 \text{ for all } \boldsymbol{y} \in C\}$. If $C \subseteq C^\perp$, a code C is called self-orthogonal and if $C = C^\perp$, C is called self-dual.

Two codes are permutation-equivalent if one can be obtained from the other by permuting coordinates. Any $\boldsymbol{Z}_4$-code is permutation-equivalent to a code with generator matrix of the form

$$G = \begin{pmatrix} I_{k_1} & A & B \\ O & 2I_{k_2} & 2D \end{pmatrix}$$

where the entries of A and D are in $\boldsymbol{Z}_2 = \{0, 1\}$ and the entries of B are in $\boldsymbol{Z}_4$. Then it contains $4^{k_1}2^{k_2}$ codewords. We say that the code C has type $4^{k_1}2^{k_2}$. It is known that if $\boldsymbol{Z}_4$-code C has type $4^{k_1}2^{k_2}$, then the dual code $C^\perp$ has type $4^{n-k_1-k_2}2^{k_2}$.

Let $n_i(\boldsymbol{a})$ be the number of components of a vector $\boldsymbol{a}$ that are congruent to i (mod 4), $i = 0, 1, 2, 3$. The Hamming weight $wt_H(\boldsymbol{a})$ of $\boldsymbol{a}$ is defined by $wt_H(\boldsymbol{a}) = n_1(\boldsymbol{a}) + n_2(\boldsymbol{a}) + n_3(\boldsymbol{a})$ and the Euclidean weight $wt_E(\boldsymbol{a})$ of $\boldsymbol{a}$ is defined by $wt_E(\boldsymbol{a}) = n_1(\boldsymbol{a}) + 4n_2(\boldsymbol{a}) + n_3(\boldsymbol{a})$.

The Hammimg distance $d_H(\boldsymbol{a}, \boldsymbol{b})$ is defined by $wt_H(\boldsymbol{a} - \boldsymbol{b})$ and the Euclidean distance $d_E(\boldsymbol{a}, \boldsymbol{b})$ is defined by $wt_E(\boldsymbol{a} - \boldsymbol{b})$.

The minimum Hamming distance d_H of a $\boldsymbol{Z}_4$-code C is

$$\min\{d_H(\boldsymbol{a}, \boldsymbol{b}) | \boldsymbol{a}, \boldsymbol{b} \in C, \boldsymbol{a} \neq \boldsymbol{b}\}$$

and the minimum Euclidean distance d_E of C is

$$\min\{d_E(\boldsymbol{a}, \boldsymbol{b}) | \boldsymbol{a}, \boldsymbol{b} \in C, \boldsymbol{a} \neq \boldsymbol{b}\}.$$

The highest minimum Hamming weights and the highest minimum Euclidean weights of Type IV self-dual codes of lengths up to 40, Type IV-I codes of length 56 and Type IV-II codes of lengths 48,56,64 were determined [2].

Klemm's code K_n is given as

$$K_n = R_n + 2P_n = 2P_n \cup (\boldsymbol{e} + 2P_n)$$

where R_n is a repetition code, P_n is its dual code, and $\boldsymbol{e}$ is the all-one vector. For $3r \leq m - 1$, $C_{m,r}$ code is given as

$$C_{m,r} = RM(r, m) + 2RM(m - r - 1, m)$$

where $RM(r, m)$ is a Reed-Muller code.

3 Self-dual $\boldsymbol{Z}_4$-codes of Type IV generated by conference matrices

If a square matrix H of order n with entries ± 1 satisfies $HH^t = nI$, then it is called an Hadamard matrix. An Hadamard matrix $H = H_0 + I$ such that $H_0^t = -H_0$ is called a skew-Hadamard matrix. The distinct rows of an Hadamard matrix are orthogonal. If we recognize the entries 1 and -1 of an Hadamard matrix H_{4m} of order $4m$ as the elements of $\boldsymbol{Z}_4$, then the $\boldsymbol{Z}_4$-code generated by rows of H_{4m} is self-orthogonal.

In this section, we give families of self-dual $\boldsymbol{Z}_4$-codes of Type IV-I and Type IV-II generated by conference matrices and skew-Hadamard matrices.

Let q be an odd prime power and $\mathrm{GF}(q)$ be a finite field with q elements. Let χ be a quadratic character of $\mathrm{GF}(q)$. We let $\chi(0) = 0$. A Paley matrix $P = (p_{ij})$ of order q is the matrix whose entry p_{ij} is defined by

$$p_{ij} = \chi(a_i - a_j)$$

where a_i and a_j $(0 \le i, j \le q-1)$ are elements of $\mathrm{GF}(q)$. Denote a conference matrix of order $q+1$ by Q, that is

$$Q = \begin{pmatrix} 0 & \boldsymbol{e} \\ \chi(-1)\boldsymbol{e}^t & P \end{pmatrix}$$

where $\boldsymbol{e}$ is the all-one vector.

The followings relations are well-known.

$$QQ^t = qI, \quad Q^t = \chi(-1)Q \tag{1}$$

where I is the unit matrix.

In what follows, we recognize the entries $1, -1$ and 0 of a matrix as the elements of $\boldsymbol{Z}_4$. We construct families of self-dual $\boldsymbol{Z}_4$-codes of Type IV-I and of Type IV-II.

Theorem 1. *Put $N = Q + 2I$. Define the matrix G_Q as follows:*

$$G_Q = \begin{pmatrix} I & N & N & I \\ O & 2I & 2(J-I) & 2J \\ O & O & 2I & 2(J-I) \end{pmatrix}$$

where J is the all-one matrix and O is the zero matrix. Then C_Q with generator matrix G_Q is a self-dual $\boldsymbol{Z}_4$-code of Type IV.

Proof. From the relations (1), we have $NN^t = (Q+2I)(Q^t+2I) = QQ^t+2(Q+Q^t) = qI$, $2NN^t+2I = O$, $2N = 2(J-I)$, $2N+2(J-I) = O$ and $2N+2n(J-I)+2J = O$.

Hence we have,

$$G_Q G_Q^t = \begin{pmatrix} I & N & N & I \\ O & 2I & 2(J-I) & 2J \\ O & O & 2I & 2(J-I) \end{pmatrix} \begin{pmatrix} I & O & O \\ N^t & 2I & O \\ N^t & 2(J-I) & 2I \\ I & 2J & 2(J-I) \end{pmatrix}$$
$$= \begin{pmatrix} 2I+2NN^t & 2N+2N(J-I)+2J & 2N+2(J-I) \\ 2N^t+2(J-I)N^t+2J & O & O \\ 2N^t+2(J-I) & O & O \end{pmatrix}$$
$$= O.$$

Since the number of codewords of C_Q is $4^{q+1}2^{2(q+1)}$, the number of codewords of the dual code $C_Q^{\perp}$ is $4^{4(q+1)-(q+1)-2(q+1)}2^{2(q+1)} = 4^{q+1}2^{2(q+1)}$. Hence C_Q is a self-dual $\boldsymbol{Z}_4$-code.

Next we shall prove C_Q is a Type IV code. Put $n = q+1$. Let $G_Q = \begin{pmatrix} G_1 \\ G_2 \\ G_3 \end{pmatrix}$ where $G_1 = (I, N, N, I)$, $G_2 = (O, 2I, 2(J-I), 2J)$ and $G_3 = (O, O, 2I, 2(J-I))$. Put $G_1 = \begin{pmatrix} \boldsymbol{u}_1 \\ \boldsymbol{u}_2 \\ \vdots \\ \boldsymbol{u}_n \end{pmatrix}$, $G_2 = \begin{pmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \\ \vdots \\ \boldsymbol{v}_n \end{pmatrix}$ and $G_3 = \begin{pmatrix} \boldsymbol{w}_1 \\ \boldsymbol{w}_2 \\ \vdots \\ \boldsymbol{w}_n \end{pmatrix}$. Then the codeword $\boldsymbol{c}$ of C_Q is written as

$$\boldsymbol{c} = \sum_{k=1}^{n} \alpha_k \boldsymbol{u}_k + \sum_{k=1}^{n} \beta_k \boldsymbol{v}_k + \sum_{k=1}^{n} \gamma_k \boldsymbol{w}_k$$

where $\alpha_k \in \boldsymbol{Z}_4$ and $\beta_k, \gamma_k \in \boldsymbol{Z}_2$ $(1 \le k \le n)$.

Let $s = |\{\alpha_k : \alpha_k = \pm 1\}|$ and $t = |\{\alpha_k : \alpha_k = 2\}|$. We may assume the first s coefficients $\alpha_1, \cdots, \alpha_s$ are odd, and the next t coefficients $\alpha_{s+1}, \cdots, \alpha_{s+t}$ are all 2, and other coefficients are all zero by permuting rows and columns of G_1. The matrices G_2 and G_3 do not change by further suitable permuting rows and columns of G_2 and G_3.

Then the codeword is written as

$$\boldsymbol{c} = \sum_{k=1}^{s} \alpha_k \boldsymbol{u}_k + \sum_{k=1}^{t} \alpha'_k \boldsymbol{u}_{k+s} + \sum_{k=1}^{n} \beta_k \boldsymbol{v}_k + \sum_{k=1}^{n} \gamma_k \boldsymbol{w}_k$$

where $\alpha_k = \pm 1, (1 \le k \le s)$ and $\alpha'_k = 2 (1 \le k \le t)$. Denote the (k, l) entry of the matrix N by $N(k, l)$. Let the vector $\boldsymbol{g}_1 = \sum_{k=1}^{s} \alpha_k \boldsymbol{u}_k + \sum_{k=1}^{t} \alpha'_k \boldsymbol{u}_k = (g_1, g_2, \cdots, g_{4n})$. Then we have

- $g_i = \alpha_i, \quad (1 \le i \le s)$,

- $g_{i+s} = \alpha'_i, \quad (1 \le i \le t),$
- $g_{i+s+t} = 0, \quad (1 \le i \le n-(s+t)),$
- $g_{i+n} = g_{i+2n} = \sum_{k=1}^{s} \alpha_k N(k,i) + \sum_{k=1}^{t} \alpha'_k N(s+k,i), \ (1 \le i \le n),$
- $g_{i+3n} = \alpha_i, \quad (1 \le i \le s),$
- $g_{i+3n+s} = \alpha'_i, \quad (1 \le i \le t),$
- $g_{i+3n+s+t} = 0, \quad (1 \le i \le n-(s+t)).$

Thus the codeword $\boldsymbol{c} = (c_1, c_2, \cdots, c_{4n})$ is given as

- $c_i = \alpha_i, \quad (1 \le i \le s),$
- $c_{i+s} = \alpha'_i, \quad (1 \le i \le t),$
- $c_{i+s+t} = 0, \quad (1 \le i \le n-(s+t)),$
- $c_{i+n} = \sum_{k=1}^{s} \alpha_k N(k,i) + \sum_{k=1}^{t} \alpha'_k N(s+k,i) + 2\beta_i, \ (1 \le i \le n),$
- $c_{i+2n} = \sum_{k=1}^{s} \alpha_k N(k,i) + \sum_{k=1}^{t} \alpha'_k N(s+k,i) + 2\beta + 2\beta_i + 2\gamma_i, (1 \le i \le n),$
- $c_{i+3n} = \alpha_i + 2\beta + 2\beta_i + 2\gamma_i, \quad (1 \le i \le s),$
- $c_{i+s+3n} = \alpha'_i + 2\beta + 2\gamma + 2\gamma_{i+s}, \quad (1 \le i \le t),$
- $c_{i+s+t+3n} = 2\beta + 2\gamma + 2\gamma_{i+s+t}, \quad (1 \le i \le n-(s+t))$

where $\beta = \sum_{k=1}^{n} \beta_k$ and $\gamma = \sum_{k=1}^{n} \gamma_k$.

We may prove the Hamming weight of the codeword $\boldsymbol{c}$ is even. Assume that $s \ne t \ne 0$. We distinguish two cases.

(1) Assume that $s \equiv 0 \pmod 2$.
Let

$$x_i = \sum_{k=1}^{s} \alpha_k N(k,i) + \sum_{k=1}^{t} \alpha'_k N(s+k,i) + 2\beta_i$$

for $1 \le i \le s$. Then

$$c_{i+n} = x_i \quad \text{and} \quad c_{i+2n} = x_i + 2\beta + 2\gamma_i$$

for $1 \le i \le s$. Notice that the number of even elements in the set $\{N(k,i) : 1 \le k \le s\}$ is just one and the other elements are all odd. It implies that

$$c_{i+n} = x_i \equiv s-1 \equiv 1 \pmod 2 \quad \text{and} \quad c_{i+2n} = x_i + 2\beta + 2\gamma_i \equiv 1 \pmod 2$$

for $1 \le i \le s$. Let

$$y_i = \sum_{k=1}^{s} \alpha_k N(k,i) + \sum_{k=1}^{t} \alpha'_k N(s+k,i) + 2\beta_i$$

for $s+1 \le i \le n$. Then

$$c_{i+n} = y_i \quad \text{and} \quad c_{i+2n} = y_i + 2\beta + 2\gamma_i$$

for $s+1 \le i \le n$. Since the elements of the set $\{N(k,i) : 1 \le k \le s\}$ are all odd for $s+1 \le i \le n$,

$$c_{i+n} = y_i \equiv s \equiv 0 \pmod 2 \quad \text{and} \quad c_{i+2n} = y_i + 2\beta + 2\gamma_i \equiv 0 \pmod 2$$

for $s+1 \le i \le n$. It is obvious that $\alpha'_k + 2\beta + 2\gamma + 2\gamma_{k+s}$ for $1 \le k \le t$ and $2\beta + 2\gamma + 2\gamma_{k+s+t}$ for $1 \le k \le n-(s+t)$ are all even. Let

$$\begin{aligned} N_1 = &|\{i :\ y_i = 2, s+1 \le i \le s+t\}| + |\{i :\ y_i + 2\beta + 2\gamma = 2, s+1 \le i \le s+t\}| \\ &+ |\{i :\ 2 + 2\beta + 2\gamma + 2\gamma_i = 2, s+1 \le i \le s+t\}| \end{aligned}$$

and

$$\begin{aligned} N_2 = &|\{i :\ y_i = 2, s+t+1 \le i \le n\}| + |\{i :\ y_i + 2\beta + 2\gamma = 2, s+t+1 \le i \le n\}| \\ &+ |\{i : 2\beta + 2\gamma + 2\gamma_i = 2, s+t+1 \le i \le n\}|. \end{aligned}$$

Notice N_1+N_2+t is the number of the components 2 of the codeword $\boldsymbol{c}$. Furthermore, for $j = 0, 2$ and $k = 0, 1$, we define

$$n_{j,k} = |\{(y_i, \gamma_i) : (y_i, \gamma_i) = (j,k), s+1 \le i \le s+t\}|,$$

and

$$n'_{j,k} = |\{(y_i, \gamma_i) : (y_i, \gamma_i) = (j,k), s+t+1 \le i \le n\}|.$$

Then

$$N_1 = \begin{cases} n_{0,0} + n_{0,1} + 3n_{2,0} + n_{2,1}, & \text{if } 2\beta = 2\gamma = 0, \\ 2n_{0,1} + 2n_{2,0} + 2n_{2,1}, & \text{if } 2\beta = 0, 2\gamma = 2, \\ n_{0,0} + n_{0,1} + 3n_{2,0} + n_{2,1}, & \text{if } 2\beta = 2, 2\gamma = 0, \\ 2n_{0,0} + 2n_{2,0} + 2n_{2,1}, & \text{if } 2\beta = 2\gamma = 2, \end{cases}$$

and

$$N_2 = \begin{cases} 2n'_{0,1} + 2n'_{2,0} + 2n'_{2,1}, & \text{if } 2\beta = 2\gamma = 0, \\ n'_{0,0} + n'_{0,1} + 3n'_{2,0} + n'_{2,1}, & \text{if } 2\beta = 0, 2\gamma = 2, \\ 2n'_{0,0} + 2n'_{2,0} + 2n'_{2,1}, & \text{if } 2\beta = 2, 2\gamma = 0, \\ n'_{0,0} + n'_{0,1} + n'_{2,0} + 3n'_{2,1}, & \text{if } 2\beta = 2\gamma = 2. \end{cases}$$

We obtain

$$N_1 + N_2 \equiv t \pmod 2,$$

from $n_{0,0}+n_{0,1}+n_{2,0}+n_{2,1}=t$ and $n'_{0,0}+n'_{0,1}+n'_{2,0}+n'_{2,1}=n-(s+t)\equiv s+t\equiv t \pmod 2$. Hence the number $N_{\boldsymbol{c}}$ of non-zero components of the codeword $\boldsymbol{c}$ is given as

$$N_{\boldsymbol{c}} \equiv 4s+t+t\equiv 0 \pmod 2$$

since the number of odd components is $s+s+s+s=4s$.

(2) Assume that $s\equiv 1 \pmod 2$.
Similarly to the argument in (1),

$$c_{i+n}=x_i\equiv s-1\equiv 0 \pmod 2 \quad \text{and} \quad c_{i+2n}=x_i+2\beta+2\gamma_i\equiv 0 \pmod 2$$

for $1\le i\le s$ and

$$c_{i+n}=y_i\equiv s\equiv 1 \pmod 2 \quad \text{and} \quad c_{i+2n}=y_i+2\beta+2\gamma_i\equiv 1 \pmod 2$$

for $s+1\le i\le n$. Let

$$M_1=|\{i: x_i=2, 1\le i\le s\}|+|\{i: x_i+2\beta+2\gamma_i=2, 1\le i\le s\}|$$

and

$$\begin{aligned} M_2=&|\{i: 2+2\beta+2\gamma+2\gamma_i=2, s+1\le i\le s+t\}|\\ &+|\{i: 2\beta+2\gamma+2\gamma_i=2, s+t+1\le i\le n\}|. \end{aligned}$$

Notice that M_1+M_2+t is the number of the components 2 of the codeword $\boldsymbol{c}$. For $j=0,2$ and $k=0,1$, we let

$$m_{j,k}=|\{(x_i,\gamma_i):(x_i,\gamma_i)=(j,k), 1\le i\le s\}|$$

and

$$u_1=|\{i:\gamma_i=1, s+1\le i\le s+t\}| \quad \text{and} \quad u_2=|\{i:\gamma_i=1, s+t+1\le i\le n\}|.$$

It is clear that $\gamma=m_{0,1}+m_{2,1}+u_1+u_2$ and $s=m_{0,0}+m_{0,1}+m_{2,0}+m_{2,1}$. Then we have

$$M_1+M_2=\begin{cases} 2m_{2,0}+m_{2,1}+m_{0,1}+t-u_1+u_2\equiv \gamma+t\equiv t \pmod 2, \\ \qquad\qquad \text{if } 2\beta=2\gamma=0, \\ 2m_{2,0}+m_{2,1}+m_{0,1}+u_1+n-(s+t)-u_2\equiv t \pmod 2, \\ \qquad\qquad \text{if } 2\beta=0,\ 2\gamma=2, \\ m_{2,0}+2m_{2,1}+m_{0,0}+u_1+n-(s+t)-u_2\equiv t \pmod 2, \\ \qquad\qquad \text{if } 2\beta=2,\ 2\gamma=0, \\ m_{2,0}+2m_{2,1}+m_{0,0}+t-u_1+u_2\equiv t \pmod 2, \\ \qquad\qquad \text{if } 2\beta=2\gamma=2. \end{cases}$$

Hence the number $N_{\boldsymbol{c}}$ of non-zero components of the codeword $\boldsymbol{c}$ is given as

$$N_{\boldsymbol{c}}=2n+t+t\equiv 0 \pmod 2$$

since the number of odd components is $s + (n - s) + (n - s) + s = 2n$.

For the case $s = 0$ and $t > 0$, we put

$$N_1 = |\{i : y_i = 2, 1 \leq i \leq n\}| + |\{i : y_i + 2\beta + 2\gamma_i = 2, 1 \leq i \leq n\}|$$

and

$$\begin{aligned} N_2 = & |\{i : 2 + 2\beta + 2\gamma + 2\gamma_i = 2, 1 \leq i \leq t\}| \\ & + |\{i : 2\beta + 2\gamma + 2\gamma_{i+t} = 2, 1 \leq i \leq n - t\}|. \end{aligned}$$

Then non-zero components of the codeword $\boldsymbol{c}$ is $N_1 + N_2 + t$. We can prove $N_1 + N_2 + t \equiv 0 \pmod 2$ similarly to the proof for the case (2). For the other cases that $s > 0, t = 0$, and $s = t = 0$, we can also prove the Hamming weight of $\boldsymbol{c}$ is even.

Theorem 2. *The $\boldsymbol{Z}_4$-code C_Q is a Type IV-II code if $q \equiv 3 \pmod 4$ and a Type IV-I code if $q \equiv 1 \pmod 4$. Furthermore C_Q contains the all-one vector.*

Proof. The Euclidean weight of every row of G_1 is $2(q+1)+2\cdot 4 = 2q+2$. It implies that $2q+2 \equiv 0 \pmod 8$ if $q \equiv 3 \pmod 4$ and $2q+2 \equiv 4 \pmod 8$ if $q \equiv 1 \pmod 4$. The Euclidean weight of every row of G_1 and G_2 is $8(q+1)$ and $4(q+1)$ respectively. Hence C_Q is Type IV-II if $q \equiv 3 \pmod 4$ and a Type IV-I code if $q \equiv 1 \pmod 4$.

Let $\boldsymbol{x} = \sum_{i=1}^{n} \boldsymbol{u}_i + \sum_{i=1}^{n} \boldsymbol{v}_i$, that is the sum of all rows of G_1 and of G_2. We see that $\sum_{i=1}^{n} \boldsymbol{u}_i = (\boldsymbol{e}, 3\boldsymbol{e}, 3\boldsymbol{e}, \boldsymbol{e})$ and $\sum_{i=1}^{n} \boldsymbol{v}_i = (\boldsymbol{0}, 2\boldsymbol{e}, 2\boldsymbol{e}, \boldsymbol{0})$. It yields $\boldsymbol{x} = \boldsymbol{e}$.

We give the minimum Hamming distance and the minimum Euclidean distance of C_Q.

Corollary 1. *The minimum Hamming distance of C_Q is 2 and the minimum Euclidean distance is 8.*

Proof. Let $\boldsymbol{y} = \boldsymbol{v}_n + \sum_{i=1}^{n} \boldsymbol{w}_i$, that is the sum of the last row of G_2 and all rows of G_3. Then

$$\begin{aligned} \boldsymbol{y} &= (\boldsymbol{0}, 2, 0, \cdots, 0, 0, 2, \cdots, 2, 2\boldsymbol{e}) + (\boldsymbol{0}, \boldsymbol{0}, 2\boldsymbol{e}, 2\boldsymbol{e}) \\ &= (\boldsymbol{0}, 2, 0, \cdots, 0, 2, 0, \cdots, 0, \boldsymbol{0}). \end{aligned}$$

It guarantees there exists a codeword with $wt_H(\boldsymbol{y}) = 2$ and $wt_E(\boldsymbol{y}) = 8$. Hence the minimum Hamming distance is 2 and the minimum Euclidean distance is 8 if $q \equiv 3 \pmod 4$. If $s \equiv 0 \pmod 2$ and $s > 0$, then 4-tuple $\alpha_i, x_i, x_i + 2\beta + 2\gamma_i$ and $\alpha_i + 2\beta + 2\gamma + 2\gamma_i$ are odd for $1 \leq i \leq s$. Thus $wt_E(\boldsymbol{c}) \geq 8$. If $s = 0$ and $t > 0$, 2-tuple α'_i and $\alpha'_i + 2\beta + 2\gamma + 2\gamma_i, (1 \leq i \leq t)$ are 2. Then $wt_E(\boldsymbol{c}) \geq 2 \cdot 4$. If $s \equiv 1 \pmod 2$, the number of the components 2 is even, that is $wt_E(\boldsymbol{c}) \geq 2 \cdot 4$. It leads to the case $s = 0$ and $t = 0$ if there exists a codeword with $wt_E(\boldsymbol{c}) = 4$. It means the codeword $\boldsymbol{c}$ has only one component 2. It contradicts C_Q is a Type IV. Hence the minimum Euclidean distance of C_Q is 8.

It is well known that $Q + I$ is a skew-Hadamard matrix if $q \equiv 3 \pmod 4$. So we obtain the following theorem.

Theorem 3. *Let $H = H_0 + I$ be a skew-Hadamard matrix of order $4n$. Put $N = H + I$. We define*

$$G_S = \begin{pmatrix} I & N & N & I \\ O & 2I & 2(J-I) & 2J \\ O & O & 2I & 2(J-I) \end{pmatrix}.$$

Then the $\boldsymbol{Z}_4$-code C_S with generator matrix G_S is a self-dual code of Type IV-II. The minimum Hamming distance is 2 and the minimum Euclidean distance is 8. If H is a regular skew-Hadamard matrix, then C_S contains the all-one vector.

Proof. Since H is a skew-Hadamard matrix, then $NN^t = HH^t + H + H^t + I = (4n+3)I$. We prove C_S is a self-dual $\boldsymbol{Z}_4$-code of Type IV and the Euclidean weight of every row of G_S is divisible by 8 similarly to the proof of Theorem 1. We establish that the minimum Hamming distance is 2 and the minimum Euclidean distance is 8 similarly to the proof of Corollary 1. If H is a regular skew-Hadamard matrix, then the vector $\boldsymbol{x}$ whose component is a column sum of $G_1 = (I, N, N, I)$ is $(\boldsymbol{e}, \boldsymbol{e}, \boldsymbol{e}, \boldsymbol{e})$ or $(\boldsymbol{e}, 3\boldsymbol{e}, 3\boldsymbol{e}, \boldsymbol{e})$. Let the vector $\boldsymbol{y} = (\mathbf{0}, 2\boldsymbol{e}, 2\boldsymbol{e}, \mathbf{0})$ whose component is a column sum of $G_2 = (O, 2I, 2(J-I), 2J)$. Then we obtain the all-one vector $\boldsymbol{e}$ by adding $\boldsymbol{y}$ and $\boldsymbol{x}$ if necessary.

4 Self-dual $\boldsymbol{Z}_4$-codes of Type IV generated by bordered skew-Hadamard matrices

In this section, we give an another family of self-dual $\boldsymbol{Z}_4$-codes of Type IV-I. By using matrices of order $4n+1$ with borders, we construct $\boldsymbol{Z}_4$-codes of length $4(4n+1)$. Denote a skew-Hadamard matrix of order $4n$ by H. We define the matrices N, X, Y and Z of order $4n+1$ as follows.

$$N = \begin{pmatrix} 1 & 2\boldsymbol{e} \\ 2\boldsymbol{e}^t & H+I \end{pmatrix}, \quad X = \begin{pmatrix} 0 & \mathbf{0} \\ \mathbf{0} & 2(J-I) \end{pmatrix},$$

$$Y = \begin{pmatrix} 2 & \mathbf{0} \\ \mathbf{0}^t & 2(J-I) \end{pmatrix}, \quad Z = \begin{pmatrix} 2 & \mathbf{0} \\ \mathbf{0}^t & 2J \end{pmatrix}.$$

Theorem 4. *We define*

$$G_H = \begin{pmatrix} I & N & N & I \\ O & 2I & X & Z \\ O & O & 2I & Y \end{pmatrix}.$$

Then the $\boldsymbol{Z}_4$-code C_H with generator matrix G_H is a Type IV-I self-dual code.

Proof. We verify that $G_H G_H^t = O$. It is easy to see that $2\boldsymbol{e}(H+I) = 2\boldsymbol{e}$, $(H+I)(H^t+I) = (4n+3)I$ and $2(H+I)(J-I) = 2(J-I)^2 = 2J$. Then we have

$$NN^t = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^t & (4n+3)I \end{pmatrix}, \quad NX^t = \begin{pmatrix} 0 & \mathbf{0} \\ \mathbf{0}^t & 2I \end{pmatrix}.$$

It follows that

$$2I + 2NN^t = 2N + NX^t + Z^t = 2N + Y^t = O.$$

Thus we obtain

$$G_H G_H^t = O.$$

Since the number of codewords of C_H is $4^{(4n+1)}2^{2(4n+1)}$, the number of codewords of the dual code $C_H^\perp$ is also $4^{(4n+1)}2^{2(4n+1)}$. Hence C_H is a self-dual $\boldsymbol{Z}_4$-code. The matrix G_H is written as

$$G_H = \begin{pmatrix} 1 & \mathbf{0} & 1 & 2\boldsymbol{e} & 1 & 2\boldsymbol{e} & 1 & \mathbf{0} \\ \mathbf{0}^t & I & 2\boldsymbol{e}^t & H+I & 2\boldsymbol{e}^t & H+I & \mathbf{0}^t & I \\ 0 & \mathbf{0} & 2 & \mathbf{0} & 0 & \mathbf{0} & 2 & \mathbf{0} \\ \mathbf{0}^t & O & \mathbf{0}^t & 2I & \mathbf{0}^t & 2(J-I) & \mathbf{0}^t & 2J \\ 0 & \mathbf{0} & 0 & \mathbf{0} & 2 & \mathbf{0} & 2 & \mathbf{0} \\ \mathbf{0}^t & O & \mathbf{0}^t & O & \mathbf{0}^t & 2I & \mathbf{0}^t & 2(J-I) \end{pmatrix}.$$

The generator matrix G_H is permutation-equivalent to the following matrix

$$\overline{G}_H = \begin{pmatrix} 1 & 1 & 1 & 1 & \mathbf{0} & 2\boldsymbol{e} & 2\boldsymbol{e} & \mathbf{0} \\ 0 & 2 & 0 & 2 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ 0 & 0 & 2 & 2 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0}^t & 2\boldsymbol{e}^t & 2\boldsymbol{e}^t & \mathbf{0}^t & I & H+I & H+I & I \\ \mathbf{0}^t & \mathbf{0}^t & \mathbf{0}^t & \mathbf{0}^t & O & 2I & 2(J-I) & 2J \\ \mathbf{0}^t & \mathbf{0}^t & \mathbf{0}^t & \mathbf{0}^t & O & O & 2I & 2(J-I) \end{pmatrix}.$$

Since $\overline{G}_H$ contains the matrix G_S in Theorem 3 as a submatrix, the Hamming weight of the codeword is even, which is a linear combination of the rows of lower block of $\overline{G}_H$. It is clear that the Hamming weight of the codeword which is a linear combination of upper 3 rows of $\overline{G}_H$ is even. It holds that the Hamming weight of the linear combination of $\overline{G}_H$ is even.

The length of C_H is $4(4n+1)+4 \equiv 4 \pmod 8$. Hence C_H is a Type IV-I code.

Corollary 2. *The minimum Hamming distance of C_H is 2 and the minimum Euclidean distance is 8.*

Proof. Let $\boldsymbol{y}$ be as in Corollary 1 such that $wt_H(\boldsymbol{y}) = 2$ and $wt_E(\boldsymbol{y}) = 8$. Thus the sum of the last row $(0,0,0,0,\mathbf{0},2,0,\ldots,0,0,2,\ldots,2,2\boldsymbol{e})$ of 5th block $(\mathbf{0}^t,\mathbf{0}^t,\mathbf{0}^t,\mathbf{0}^t, 2I, 2(J-I), 2J)$ and all rows of 6th block $(\mathbf{0}^t,\mathbf{0}^t,\mathbf{0}^t,\mathbf{0}^t,O,O,2I,2(J-I))$ gives the codeword of C_H such that the Hamming weight is 2 and the Euclidean weight is 8. Similarly to the proof of Corollary 1, we obtain that the minimum Hamming weight of C_H is 2 and the minimum Euclidean weight of C_H is 8.

5 Numerical results

We list the Hamming weight distributions of Klemm's code K_{2^4}, $C_{4,1}$ code and C_Q code of length 2^4.

Hamming weight	Klemm's code	$C_{4,1}$ code	C_Q code
0	1	1	1
2	120		8
4	1820	140	252
6	8008	448	952
8	12870	1350	2118
10	8008	13888	13496
12	1820	33740	31612
14	120	13440	12552
16	32769	2529	4545

The highest minimum Hamming weights and the highest minimum Euclidean weights of Type IV self-dual codes of lengths up to 40, Type IV-I codes of length 56 and Type IV-II codes of lengths 48,56,64 were determined [2]. The self-dual code C_H of lengths 20 and 36 in Theorem 4 have the highest minimum Hamming and Euclidean weights. Furthermore, the self-dual code C_Q of length 24 in Theorem 1 has the highest minimum Hamming and Euclidean weight.

References

[1] A. Bonnecaze, P. Solé, C. Bachoc and B. Mourrain, Type II codes over $\boldsymbol{Z}_4$, *IEEE Trans. Inform. Theory* **43** (1997), 969–976.

[2] S. Bouyuklieva and M. Harada, On Type IV self-dual codes over $\boldsymbol{Z}_4$, *Discrete Math.* **247** (2002), 25–50.

[3] C. Charnes, Hadamard matrices, self-dual codes over the integers modulo 4 and their Gray images, in: *Proc. SETA'98*, Discrete Math. and Theoretical Computer Science, Springer-Verlag, Berlin, 1999, pp. 171–183.

[4] C. Charnes and J. Seberry, Weighing matrices and self-orthogonal quaternary codes, *J. Combin. Math. Combin. Comput.* **44** (2003), 85–95.

[5] S.T. Dougherty, P. Gaborit, M. Harada, A. Munemasa and P. Solé, Type IV self-dual codes over rings, *IEEE Trans. Inform. Theory* **45** (1999), 2345–2360.

[6] J. Fields, P. Gaborit, J.S. Leon and V. Pless, All self-dual $\boldsymbol{Z}_4$ of length15 or less are known, *IEEE Trans. Inform. Theory* **44** (1998), 311–321.

[7] A.R. Hammons, Jr. P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, The $\boldsymbol{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* **40** (1994), 301–319.

[8] M. Harada and A. Munemasa, Classification of Type IV self-dual $\boldsymbol{Z}_4$-codes of length 16, *Finite Fields and their Applications* **6** (2000), 244–254.

[9] W.C. Huffman, On the classification and enumeration of self-dual codes, *Finite Fields and their Applications* **11** (2005), 451–490.

(Received 31 Aug 2007)