## Some Results on Type IV Codes Over $\boldsymbol{Z}_{\mathbf{4}}$

Stefka Bouyuklieva


#### Abstract

Dougherty, Gaborit, Harada, Munemasa, and Solé have previously given an upper bound on the minimum Lee weight of a Type IV self-dual $\boldsymbol{Z}_{4}$-code, using a similar bound for the minimum distance of binary doubly even self-dual codes. We improve their bound, finding that the minimum Lee weight of a Type IV self-dual $\boldsymbol{Z}_{4}$-code of length $\boldsymbol{n}$ is at most $4\lfloor n / 12\rfloor$, except when $n=4$, and $n=8$ when the bound is 4 , and $n=16$ when the bound is 8 . We prove that the extremal binary doubly even self-dual codes of length $n \geq 24, n \neq 32$ are not $Z_{4}$-linear. We classify Type IV-I codes of length 16. We prove that all Type IV codes of length 24 have minimum Lee weight 4 and minimum Hamming weight 2, and the Euclidean-optimal Type IV-I codes of this length have minimum Euclidean weight 8.


Index Terms-Type IV codes over rings, self-dual codes, $\boldsymbol{Z}_{4}$-linearity.

## I. Introduction

A binary code is said to be $Z_{4}$-linear if it is the Gray image of a linear $Z_{4}$-code. In [7], Fields and Gaborit have shown that any extremal doubly even self-dual code of length 48 is not $Z_{4}$-linear, and the putative extremal doubly even self-dual codes of lengths 72 and 96 cannot be constructed as the Gray images of linear codes over $Z_{4}$. In this correspondence, we prove that no doubly even self-dual $[n, n / 2,4\lfloor n / 24\rfloor+4]$ code for $n \geq 24, n \neq 32$, is $Z_{4}$-linear.

Type IV self-dual codes over $Z_{4}$ have been introduced in [5] as self-dual codes with even Hamming weights. The authors proved that the Gray image of such a code is a binary doubly even self-dual code. Using the well-known bound for this type of binary codes, proven by Mallows and Sloane [11], they have shown that the minimum Lee weight $d_{L}$ of a Type IV $Z_{4}$-code of length $n$ is bounded by

$$
d_{L} \leq 4\left(1+\left\lfloor\frac{n}{12}\right\rfloor\right)
$$

We prove that no Type IV self-dual $Z_{4}$-code of length $n \geq 12, n \neq$ 16 , and minimum Lee weight $4\lfloor n / 12\rfloor+4$ exists. This result improves the bound from [5].

Theorem 1.1: If $C$ is a Type IV $Z_{4}$-code of length $n \geq 12, n \neq 16$, and minimum Lee weight $d_{L}$ then

$$
d_{L} \leq 4\left\lfloor\frac{n}{12}\right\rfloor
$$

For the other minimum weights, we prove the following theorem.
Theorem 1.2: If $C$ is a Type IV $Z_{4}$-code with minimum Lee weight $d_{L}$, minimum Hamming weight $d_{H}$, and minimum Euclidean weight $d_{E}$, then

$$
d_{H}=\frac{1}{2} d_{L} \quad d_{E} \leq 2 d_{L}
$$

[^0]A Type IV-I (resp., Type IV-II) code $C$ is Lee-optimal, Euclideanoptimal, or Hamming-optimal if $C$ has highest minimum Lee, Euclidean, and Hamming weight among all Type IV-I (resp., Type IV-II) codes of that length, respectively. Theorem 1.2 shows that a Type IV code is Lee-optimal iff it is Hamming-optimal.
The highest minimum Lee, Euclidean, and Hamming weights of length $n$ are denoted by $d_{L}(n), d_{E}(n)$, and $d_{H}(n)$, respectively. In [5], the parameters $d_{L}(n), d_{E}(n)$, and $d_{H}(n)$ for lengths up to 24 have been listed in two tables (for Type IV-I and Type IV-II codes). For Type IV-I, it was not known if $d_{H}(16)=2$ or $4, d_{E}(16)=4$ or 8 , $d_{L}(24)=4$ or 8 , and $d_{E}(24)=8$ or 12 . We prove that all Type IV-I codes of length 16 have minimum Hamming weight 2, but there exists a code of this length with minimum Euclidean weight 8 . Table I is the updated table for Type IV-I codes.
To prove the result for Type IV-I codes of length 16, we give the complete classification of these codes.

Definitions and preliminary results used in this correspondence are given in Section II. Nonlinearity of the $Z_{4}$ extremal doubly even self-dual codes of length $n \geq 24, n \neq 32$ and Theorem 1.1 are proved in Section III. In Section IV, we consider the connection between the minimum distances of the residue and torsion codes of a Type IV code. The classification of Type IV-I codes of length 16 is given in Section V. In the last section, we prove that the highest minimum Lee, Hamming, and Euclidean weights for Type IV-I code of length 24 are 4,2 , and 8 , respectively.

## II. PreLiminaries

A linear code $C$ of length $n$ over $Z_{4}$ is an additive submodule of $Z_{4}^{n}$. There are three different weights for codes over $Z_{4}$, namely, the Hamming weight, the Lee weight, and the Euclidean weight. The Lee weights of the elements $0,1,2$, and 3 of $Z_{4}$ are $0,1,2$, and 1 , respectively, and the Lee weight of a codeword is the rational sum of the Lee weights of its components. The Euclidean weights for the elements of $Z_{4}$ are $0,1,4,1$, respectively. The Euclidean weight of a codeword is the rational sum of the Euclidean weights of its components. The usual Hamming weight of binary or quaternary vector $v$ is the number of its nonzero components, and it is denoted by $w_{H}(v)$. In the case where all the codewords of a binary code have weight a multiple of 4 the code is said to be doubly even.
We say that two $Z_{4}$-codes are equivalent if one can be obtained from the other by permuting the coordinates and (if necessary) interchanging two elements 1 and 3 of certain coordinates. Codes differing by only a permutation of coordinates are called permutation-equivalent.
Any code over $Z_{4}$ is permutation-equivalent to a code $C$ with a generator matrix of the form

$$
\left(\begin{array}{ccc}
I_{k_{1}} & A & B_{1}+2 B_{2}  \tag{1}\\
O & 2 I_{k_{2}} & 2 D
\end{array}\right)
$$

where $A, B_{1}, B_{2}$, and $D$ are $(1,0)$-matrices. We say that a code with generator matrix (1) has type $4^{k_{1}} 2^{k_{2}}$. The binary $\left[n, k_{1}\right]$ code $C_{1}$ with generator matrix

$$
\left(\begin{array}{lll}
I_{k_{1}} & A & B_{1} \tag{2}
\end{array}\right)
$$

is called the residue code of $C$. The binary $\left[n, k_{1}+k_{2}\right]$ code $C_{2}$ with generator matrix

$$
\left(\begin{array}{ccc}
I_{k_{1}} & A & B_{1}  \tag{3}\\
O & I_{k_{2}} & D
\end{array}\right)
$$

TABLE I
The Highest Minimum Weights for Type IV-I $Z_{4}$-Codes

| Length | $d_{L}(n)$ | Codes | $d_{H}(n)$ | Codes | $d_{E}(n)$ | Codes |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 4 | 4 | $\mathcal{D}_{4}^{\oplus}[5]$ | 2 | $\mathcal{D}_{4}^{\oplus}[5]$ | 4 | $\mathcal{D}_{4}^{\Theta}[5]$ |
| 8 | 4 | $\mathcal{D}_{4}^{\oplus^{2}}[5]$ | 2 | $\mathcal{D}_{4}^{\oplus^{2}}[5]$ | 4 | $\mathcal{D}_{4}^{\oplus^{2}}[5]$ |
| 12 | 4 | all codes | 2 | all codes $[5]$ | 8 | $K_{12}[5]$ |
| 16 | 4 | the six codes | 2 | the six codes | 8 | $C^{(3)}$ and $C^{(6)}$ |
| 20 | 4 | all codes $[5]$ | 2 | all codes $[5]$ | 8 | $K_{20}[5]$ |
| 24 | 4 | all codes | 2 | all codes | 8 | $K_{12} \oplus K_{12}$ |

is called the torsion code of the $Z_{4}$-code
Several weight enumerators are associated with a code over $Z_{4}$. In this correspondence, we deal with the symmetrized weight enumerators (swe), given by

$$
\operatorname{swe}_{C}(b, c)=\sum_{x \in C} b^{n_{1}(x)+n_{3}(x)} c^{n_{2}(x)}
$$

where $n_{i}(x)$ is the number of components $i$ of $x$.
We define an inner product in $Z_{4}^{n}$ by

$$
x \cdot y=x_{1} y_{1}+\cdots+x_{n} y_{n}(\bmod 4)
$$

The dual code $C^{\perp}$ of $C$ is defined as

$$
C^{\perp}=\left\{x \in Z_{4}^{n} \mid x \cdot y=0 \forall y \in C\right\} .
$$

$C$ is self-dual if $C=C^{\perp}$. Note that self-dual codes over $Z_{4}$ exist for all $n>0$.

Self-dual codes over $Z_{4}$ with even Hamming weights are called Type IV. Basic properties of Type IV codes over rings of order 4 are proved in [5].

Theorem 2.1 [5]: Let $C$ be a code over $Z_{4}$. Suppose that $C_{1}$ and $C_{2}$ have generator matrices given by (2) and (3), respectively. If $C$ is Type IV, then there exists a unique $(1,0)$-matrix $B$ such that

$$
\left(\begin{array}{ccc}
I_{k_{1}}+2 B & A & B_{1}  \tag{4}\\
O & 2 I_{k_{2}} & 2 D
\end{array}\right)
$$

is a generator matrix of $C$. Moreover, we have

1) $C_{2}=C_{1}^{\perp}$,
2) the residue code $C_{1}$ contains the all-ones vector, and

$$
w_{H}(x * y) \equiv 0(\bmod 4)
$$

for any $x$ and $y \in C_{1}$,
3) the number of 2 's in each row of $I_{k_{1}}+2 B$ is even, and the matrix $B$ is symmetric.
Conversely, if $C_{1}$ and $C_{2}$ are binary codes with generator matrices given by (2) and (3), respectively, and if the conditions 1 )-3) are satisfied, then the $Z_{4}$-code $C$ with generator matrix (4) is a Type IV code.

We recall that the Gray map $\phi$ is a distance-preserving map from $Z_{4}^{n}$ (Lee distance) to $Z_{2}^{2 n}$ (Hamming distance). Therefore, the minimum (Hamming) weight of the binary Gray image $\mathcal{C}=\phi(C)$ is the minimum Lee weight of the $Z_{4}$-code $C$. We will use the following definition of the Gray map. Two maps $\beta$ and $\gamma$ from $Z_{4}$ to $Z_{2}$ are defined as

| $c$ | $\beta(c)$ | $\gamma(c)$ |
| :---: | :---: | :---: |
| 0 | 0 | 0 |
| 1 | 0 | 1 |
| 2 | 1 | 1 |
| 3 | 1 | 0 |

and the Gray map $\phi: Z_{4}^{n} \rightarrow Z_{2}^{2 n}$ is given by

$$
\phi(c)=(\beta(c), \gamma(c)), \quad c \in Z_{4}^{n} .
$$

We will use a linearity condition which is equivalent to [9, Theorem 5].

Theorem 2.2: If $C$ is a $Z_{4}$-code, its Gray image $\phi(C)$ is linear if and only if $x_{1}, x_{2} \in C_{1} \Rightarrow x_{1} * x_{2} \in C_{2}$, where "*" stands for the Hadamard product.

To prove some restrictions on the minimum distance of the residue code, we need the following theorem.

Theorem 2.3 [6]: If $C$ is a $Z_{4}$-code whose Gray image is a linear binary code then the codewords $u_{1}, u_{2}, \ldots, u_{t} \in C_{1}$ for which $w_{H}\left(u_{i}\right)<2 d_{2}, i=1, \ldots, t$, have disjoint support, and for each codeword $u \in C_{1}$ we have $u * u_{i}=0$ or $u * u_{i}=u_{i}, i=1, \ldots, t$.

For Type IV self-dual $Z_{4}$-codes we have
Theorem 2.4 [5]: If $C$ is a Type IV $Z_{4}$-code then its Gray image $\phi(C)$ is a doubly even self-dual binary code.

Self-dual codes over $Z_{4}$ with the property that all Euclidean weights are divisible by eight are called Type II. Self-dual codes which are not Type II are called Type I.

Proposition 2.5 [5]: A Type IV code $C$ over $Z_{4}$ is Type IV-II if and only if all the Hamming weights of $C_{1}$ are multiples of 8 .

## III. On the Non- $Z_{4}$-Linearity of Extremal Type II Codes

Let $\mathcal{C}$ be an extremal binary doubly even self-dual code of length $2 n$ which is the Gray image of a linear $Z_{4}$-code $C$. Since $\phi(-c)=$ $(\gamma(c), \beta(c))$, it follows that $\mathcal{C}$ is fixed under the "swap" map $\sigma$ that interchanges the left and right halves of each codeword. In other words

$$
\sigma=(1, n+1)(2, n+2) \cdots(n, 2 n)
$$

is an automorphism of $\mathcal{C}$. Let $C_{1}$ and $C_{2}$ be the residue and the torsion codes of the $Z_{4}$-code $C$. With $\mathcal{C}_{\sigma}$, we denote the fixed subcode of $\mathcal{C}$ under $\sigma$, namely, $\mathcal{C}_{\sigma}=\{v \in \mathcal{C}: \sigma(v)=v\}$. Obviously, $v \in \mathcal{C}_{\sigma}$ iff $v$ is a codeword in $\mathcal{C}$ and $v=\left(v_{1}, v_{2}, \ldots, v_{n}, v_{1}, v_{2}, \ldots, v_{n}\right)$. If $\pi$ is the map from $\mathcal{C}_{\sigma}$ to $Z_{2}^{n}$ defined by $\pi(v)=\left(v_{1}, v_{2}, \ldots, v_{n}\right)$, then $C_{2}=\pi\left(\mathcal{C}_{\sigma}\right)$. For the code $C_{1}$ we have $C_{1}=\psi(\mathcal{C})$ where $\psi: Z_{2}^{2 n} \rightarrow Z_{2}^{n}$ is defined by

$$
\psi(v)=\left(v_{1}+v_{n+1}, v_{2}+v_{n+2}, \ldots, v_{n}+v_{2 n}\right) .
$$

Theorem 3.1 [2]: If $\mathcal{C}$ is a binary self-dual code of length $2 n$ with an automorphism $\sigma$ of order 2 without fixed points then $C_{1}$ is a selforthogonal code of length $n$ and $C_{2}$ is its dual code.

Corollary 3.2: If $\mathcal{C}$ is a binary doubly even self-dual code of length $2 n$ with an automorphism $\sigma$ of order 2 without fixed points then $C_{1}$ contains the all-ones vector.

Proof: Since all weights in $\mathcal{C}_{\sigma}$ are divisible by four, all weights in $C_{2}$ are even and so $\mathbf{1} \in C_{1}=C_{2}^{\perp}$.

Let $n=12 m+4 r, r=0,1,2$, and let the minimum distance of $\mathcal{C}$ be $4 m+4$. Then the minimum distance of $C_{2}$ has to be at least $2 m+2$.

Corollary 3.3: If $\mathcal{C}$ is an extremal doubly even self-dual code of length $2 n=24 m+8 r \geq 24$ which is $Z_{4}$-linear, then the minimum distance of $C_{1}$ is at least $4 m+4$.

Proof: Let $u_{1}, u_{2}, \ldots, u_{t} \in C_{1}$ be the codewords for which $w_{H}\left(u_{i}\right)<4 m+4, i=1, \ldots, t$. If $t \geq 1$, without loss of generality, we can take $u_{1}=(1 \cdots 10 \cdots 0)$ with $4 m+4>w_{H}\left(u_{1}\right) \geq 2 m+2 \geq 4$. According to Theorem 2.3, the code $C_{1}$ has a generator matrix with first row $u_{1}$ of the form

$$
G_{1}=\left(\begin{array}{cc}
11 \cdots 11 & 00 \cdots 00 \\
0 & G_{1}^{\prime}
\end{array}\right)
$$

It follows that $(110 \cdots 0) \in C_{1}^{\perp}=C_{2}$ which contradicts the minimum distance of $C_{2}$. Hence, $t=0$ and the minimum distance of $C_{1}$ is at least $4 m+4$.

Theorem 3.4: The extremal doubly even self-dual codes of length $n \geq 24, n \neq 32$, are not $Z_{4}$-linear.

Proof: Let $C$ be a $Z_{4}$-linear doubly even self-dual binary code of length $24 m+8 r, r \in\{0,1,2\}, m \geq 1$, and minimum weight $d=$ $4 m+4$. Then, $C_{1}$ is a self-orthogonal [ $\left.12 m+4 r, s, d_{1} \geq 4 m+4\right]$, and its dual code $C_{2}$ has length $12 m+4 r$, dimension $12 m+4 r-s \geq 6 m+2 r$, and minimum distance at least $2 m+2$. Using the Griesmer bound [2], we have

$$
\begin{aligned}
12 m+4 r & \left.\left.\geq \sum_{i=0}^{12 m+4 r-s-1}\right\rceil \frac{2 m+2}{2^{i}}\right\rceil \\
& \left.=3 m+3+\sum_{i=2}^{12 m+4 r-s-1}\right\rceil \frac{m+1}{2^{i-1}}\lceil \\
& \left.=3 m+3+\sum_{i=1}^{12 m+4 r-s-2}\right\rceil \frac{m+1}{2^{i}}\lceil.
\end{aligned}
$$

Let $2^{l}<m+1 \leq 2^{l+1}$ and $\left.A=\sum_{i=1}^{l}\right\rceil \frac{m+1}{2^{i}}\lceil$. Obviously

$$
\begin{aligned}
A & \left.\geq \sum_{i=1}^{l}\right\rceil \frac{2^{l}+1}{2^{i}}\left\lceil=\sum_{i=1}^{l}\right\rceil 2^{l-i}+\frac{1}{2^{i}}\lceil \\
& =\sum_{i=1}^{l}\left(2^{l-i}+1\right)=2^{l}-1+l \Rightarrow A-l \geq 2^{l}-1 .
\end{aligned}
$$

Since $12 m+4 r-s-2 \geq 6 m+2 r-2 \geq 6 \cdot 2^{l}+2 r-2>l$

$$
\begin{aligned}
12 m+4 r & \geq 3 m+3+A+12 m+4 r-s-2-l \\
& =15 m+4 r+1+A-l-s \\
& \Rightarrow s \geq 3 m+1+A-l>3 .
\end{aligned}
$$

Let $x, y \in C_{1}$ and $x * y=0$. Then

$$
\begin{aligned}
w_{H}(\mathbf{1}+x+y) & =12 m+4 r-w_{H}(x)-w_{H}(y) \\
& \leq 12 m+4 r-2(4 m+4)=4 m+4 r-8 \leq 4 m
\end{aligned}
$$

and so $y=1+x$. Hence, $C_{1}$ has a generator matrix of the form

$$
G_{1}=\left(\begin{array}{cc}
00 \cdots 00 & 11 \cdots 11 \\
11 \cdots 11 & 00 \cdots 00 \\
x_{3} & y_{3} \\
\cdots & \cdots \\
x_{s} & y_{s}
\end{array}\right)
$$

where the vectors $\mathbf{1}, x_{3}, \ldots, x_{s}$ of length $d_{1}$ are linearly independent. Since $s>3$ and $C_{1}$ contains the all-ones vector, its minimum distance $d_{1}$ is at most $6 m+2 r$. According to Theorem 2.2

$$
\left(x_{i}, y_{i}\right) *(1,0)=\left(x_{i}, 0\right) \in C_{1}, \quad i=3, \ldots, s
$$

It follows that the vectors $(\mathbf{1}, 0),\left(x_{3}, 0\right), \ldots,\left(x_{s}, 0\right)$ generate a subcode of $C_{2}$ with dimension $s-1$ and minimum distance at least $2 m+2$. Hence the vectors 1, $x_{3}, \ldots, x_{s}$ generate a $\left[d_{1}, s-1, \geq 2 m+2\right]$ code. Using the Griesmer bound, we have

$$
\begin{aligned}
d_{1} & \left.\left.\geq \sum_{i=0}^{s-2}\right\rceil \frac{2 m+2}{2^{i}}\right\rceil \\
& \left.=3 m+3+\sum_{i=2}^{s-2}\right\rceil \frac{2 m+2}{2^{i}}\lceil \\
& \left.=3 m+3+\sum_{i=1}^{s-3}\right\rceil \frac{m+1}{2^{i}}\lceil
\end{aligned}
$$

Since $s \geq 3 m+1+A-l$, we have $s-3>3 \cdot 2^{l}+1+2^{l}-1=4 \cdot 2^{l}>l$ and, therefore,

$$
\begin{aligned}
d_{1} & \geq 3 m+3+A+s-3-l \\
& \geq 3 m+A-l+3 m+1+A-l=6 m+1+2(A-l)
\end{aligned}
$$

We consider the following three cases.

1) $l \geq 2$. Then

$$
A-l \geq 2^{l}-1 \geq 3 \Rightarrow d_{1} \geq 6 m+7>6 m+2 r
$$

a contradiction
2) $l=1$. Then $4 \geq m+1>2$ and $m=2$ or 3 . It follows that

$$
A-l=\rceil \frac{m+1}{2}\left\lceil-1=1 \Rightarrow d_{1} \geq 6 m+3 .\right.
$$

If $r=0$ or 1 , we have $d_{1}>6 m+2 r$. Let $r=2$. Then $C_{1}$ must be a $[12 m+8, s \geq 3 m+2,6 m+4]$ code. If $m=2, C_{1}$ will be a binary code of length 32 , dimension at least 8 , and minimum distance 16. But codes with these parameters do not exist [1]. In the case $m=3, C_{1}$ is a binary $[44, s \geq 11,22]$ code, which is impossible.
3) $l=0$. In this case, $2 \geq m+1>1$ and $m=1$. It follows that $A-l=0$ and $d_{1} \geq 6 m+1=7$, but $d_{1}$ is even and so $d_{1}$ is at least 8 . If $r=0$, we have $d_{1}>6 \mathrm{~m}$, which is a contradiction. When $r=2, C_{2}$ should be a $[20,20-s, \geq 4]$ code and hence $s \geq 6$ [1]. It follows that $C_{1}$ is a [20,s $\geq 6, d_{1}=8$ or 10] code. According to Brouwer's table, $d_{1}=8$ and $s=6,7$, or 8 . So the vectors $1, x_{3}, \ldots, x_{s}$ generate a $\left[d_{1}=8, s-1 \geq 5, \geq 4\right]$ code. But codes with these parameters do not exist.

In the case $r=1, \mathcal{C}$ is a doubly even self-dual $[32,16,8]$ code. There are five inequivalent codes of this type. It is proved that the code $C 82$ in [3, Table A] is the Gray image of the unique Type IV $Z_{4}$-code of length 16 and minimum Lee weight 8 (see [5]).

The extended Hamming code $e_{8}$ is the unique extremal binary doubly even self-dual code of length 8 , and it is the Gray map image of the unique Type IV $Z_{4}$-code of length 4 [5]. There are exactly two inequivalent binary doubly even $[16,8,4]$ codes, namely, $d_{16}$ and $2 e_{8}$. Both of them are $Z_{4}$-linear. The first one is the Gray map image of the unique Type IV-II $Z_{4}$-code of length 8 , and the second one of the unique Type IV-I $Z_{4}$-code of this length (see [5]).

Proof of Theorem 1.1: Let $C$ be a Type IV $Z_{4}$-code of length $n=12 m+4 r, r \in\{0,1,2\}, m>0$, and minimum Lee weight
$d_{L}=4 m+4$. Then its Gray image $\mathcal{C}=\phi(C)$ is a binary doubly even self-dual $[24 m+8 r, 12 m+4 r, 4 m+4]$ code. We proved that these codes are not $Z_{4}$-linear for $m \geq 2$ and for $m=1, r=0,2$. Hence, no Type IV $Z_{4}$-code of length $n \geq 12, n \neq 16$, with minimum Lee weight $4+4\lfloor n / 12\rfloor$ exists.
There exists a unique Type IV $Z_{4}$-code of length 16 and minimum Lee weight 8 , a unique Type IV code of length 4 , and two Type IV codes of length 8 and minimum Lee weight 4 . There are exactly four inequivalent Type IV codes of length 12 and all of them have minimum Lee weight 4 [5].

## IV. On the Residue and Torsion Codes

In this section, we present some connections between the minimum weights of a Type IV code and the minimum distances of its residue and torsion codes.

Proposition 4.1: If $C$ is Type IV $Z_{4}$-code and the minimum distance of its torsion code is $d_{2}$ then the minimum distance of its residue code $C_{1}$ is at least $2 d_{2}$.

Proof: Obviously, the minimum distance of $C_{1}$ is at least 4. This proves the proposition in the case when $d_{2}=2$.

Let $d_{2} \geq 4$ and let $u_{1}, u_{2}, \ldots, u_{t} \in C_{1}$ be the codewords for which $w_{H}\left(u_{i}\right)<2 d_{2}, i=1, \ldots, t$. If $t \geq 1$, without loss of generality, we can take $u_{1}=(1 \cdots 10 \cdots 0)$ with $w_{H}\left(u_{1}\right) \geq d_{2} \geq 4$. According to Theorem 2.3, the code $C_{1}$ has a generator matrix with first row $u_{1}$ of the form

$$
G_{1}=\left(\begin{array}{cc}
11 \cdots 11 & 00 \cdots 00 \\
0 & G_{1}^{\prime}
\end{array}\right)
$$

It follows that $(110 \cdots 0) \in C_{1}^{\perp}=C_{2}$ which contradicts the minimum distance of $C_{2}$. Hence, $t=0$ and the minimum distance of $C_{1}$ is at least $2 d_{2}$.

Corollary 4.2: There is no Type IV code of type $4^{\frac{n 2}{2}}$.
Proof: Let $C$ be Type IV code of type $4^{\frac{h_{n}^{2}}{2}}$. Hence, the residue code $C_{1}$ is a binary doubly even self-dual code of length $n$ and the torsion code $C_{2}$ coincides with $C_{1}$. Then, for the minimum distance of this code, we have $d_{2}=d_{1} \geq 2 d_{2}$ which is impossible.

Proposition 4.3: If $C$ is Type IV code and the minimum distance of its torsion code is $d_{2}$, then $d_{L}(C)=2 d_{2}, d_{H}(C)=d_{2}=\frac{1}{2} d_{L}(C)$, $d_{E}(C) \leq 4 d_{2}$.

Proof: In [13], Rains has proved that the minimum Hamming weight of any self-dual code over $Z_{4}$ is equal to the minimum distance of its torsion code. So we need to prove the result only for the minimum Lee and Euclidean weights.

Obviously, if $y \in C_{2}$ is a vector of weight $d_{2}$ then $2 y$ is a codeword in $C$ of Hamming weight $d_{2}$, Lee weight $2 d_{2}$, and Euclidean weight $4 d_{2}$. Hence, the minimum Hamming, Lee, and Euclidean weights of this code are at most $d_{2}, 2 d_{2}$, and $4 d_{2}$, respectively.
Let $n_{i}(x), i=0,1,2,3$, be the number of components of $x \in C$ that are $i$ in $Z_{4}$. Suppose that $y \in C$ and $n_{1}(y)=n_{3}(y)=0$. It is easy to see that $n_{1}(x+y)+n_{3}(x+y)=n_{1}(x)+n_{3}(x)$.

We consider a generator matrix $G$ of $C$ in the form (1). Let $x$ be a nonzero codeword from $C$. If $n_{1}(x)=n_{3}(x)=0$ then $x \in 2 C_{2}$ and $w_{H}(x) \geq d_{2}, w_{L}(x)=2 w_{H}(x) \geq 2 d_{2}$.

Now let $n_{1}(x)+n_{3}(x) \geq 1$. In this case, $x=x_{1}+x_{2}$ where $x_{1} \neq 0$ is a linear combination of some of the first $k_{1}$ rows $v_{1}, \ldots, v_{k_{1}}$ of $G$ with coefficients 1 or 3 , and $x_{2}$ is a vector from $2 C_{2}$. Then

$$
x_{1}=v_{i_{1}}+\cdots+v_{i_{s_{1}}}+3 v_{j_{1}}+\cdots+3 v_{j_{s_{2}}}
$$

where $\left\{i_{1}, \ldots, i_{s_{1}}\right\} \cap\left\{j_{1}, \ldots, j_{s_{2}}\right\}=\emptyset$ and

$$
\left\{i_{1}, \ldots, i_{s_{1}}\right\} \cup\left\{j_{1}, \ldots, j_{s_{2}}\right\} \subset\left\{1, \ldots, k_{1}\right\}
$$

It follows that $n_{1}(x)+n_{3}(x)=n_{1}\left(x_{1}\right)+n_{3}\left(x_{1}\right)$. But the number of 1 's and 3 's in this vector is equal to the number of 1 's in the binary vector $x_{1}^{\prime}=v_{i_{1}}^{\prime}+\cdots+v_{i_{s_{1}}}^{\prime}+v_{j_{1}}^{\prime}+\cdots+v_{j_{s_{2}}}^{\prime}$, where $v_{i}^{\prime}$ is the $i$ th row of the matrix (2). Since $x_{1}^{\prime}$ is a nonzero codeword in $C_{1}$, its weight is at least $d_{1}$. Hence, $n_{1}\left(x_{1}\right)+n_{3}\left(x_{1}\right) \geq d_{1}$ and

$$
\begin{aligned}
w_{H}(x) & \geq n_{1}(x)+n_{3}(x)=n_{1}\left(x_{1}\right)+n_{3}\left(x_{1}\right) \geq d_{1} \geq 2 d_{2} \\
w_{L}(x) & \geq w_{H}(x) \geq 2 d_{2} .
\end{aligned}
$$

So we proved that minimum Lee weight of $C$ is exactly $2 d_{2}$.
Theorem 1.2 follows directly from the above proposition. Using it and the bound for the minimum Lee weight of Type IV codes, we have the following.

Corollary 4.4: If $C$ is Type IV code of length $n \geq 12, n \neq 16$ then

$$
d_{H}(C) \leq 2\lfloor n / 12\rfloor .
$$

## V. Type IV Codes of Length 16

There are five inequivalent Type IV-II codes of length 16. These codes are the five codes in [12], whose residue codes have no codewords of Hamming weight 4 . Only one of them has minimum Lee weight 8 , namely, $5_{-} f 5$. This code is Lee-optimal, Euclidean-optimal, and Hamming-optimal.

Let $C$ be a Type IV-I code of length 16 . Then the residue code $C_{1}$ is a doubly even binary code of length 16 , containing the all-one vector, and satisfying the condition $w_{H}(x * y) \equiv 0(\bmod 4)$ for all $x$ and $y$ in $C_{1}$. If the minimum distance of $C_{1}$ is 8 then all codewords of $C_{1}$ except the zero and the all-ones vectors have weight 8 and $C$ is Type IV-II code. Hence, the minimum distance of $C_{1}$ is 4 and its dimension $k_{1}$ is at least 2 . Let $x \in C_{1}$ be a codeword of weight 4 . Up to equivalence, $x=(1111000000000000)$. Then $C_{1}$ has a generator matrix of the form

$$
G_{1}=\left(\begin{array}{cc}
1111 & 00 \cdots 00 \\
0000 & G_{1}^{\prime}
\end{array}\right)
$$

where $G_{1}^{\prime}$ generates a doubly even binary $\left[12, k_{1}-1, \geq 4\right]$ code. We consider three cases.

1) $k_{1}=2$. Then

$$
G_{1}=\binom{1111000000000000}{0000111111111111}
$$

and since $C_{1}$ satisfies the conditions of Theorem 2.1, the code $C$ with a generator matrix
$\left(\begin{array}{c}1111000000000000 \\ 0000111111111111 \\ 2200000000000000 \\ 2020000000000000 \\ 0000220000000000 \\ 0000202000000000 \\ \cdots \\ 0000200000000020\end{array}\right)$
is the unique Type IV-I code of length 16 of type $4^{2} 2^{12}$. For this code, $d_{H}=2$ and $d_{E}=4$. We denote it by $C^{(1)}$.
2) $k_{1}=3$. In this case, $C_{1}$ contains a codeword $y \neq x$ of weight 4. Up to equivalence, $y=(0000111100000000)$. Then

$$
G_{1}=\left(\begin{array}{l}
1111000000000000 \\
0000111100000000 \\
0000000011111111
\end{array}\right)
$$

and $C$ is equivalent to a code with generator matrix
$\left(\begin{array}{c}1 a a 1100000000100 \\ a 1 a 0011000000010 \\ a a 10000111111001 \\ 0002000000000200 \\ 0000200000000200 \\ 0000020000000020 \\ 0000002000000020 \\ 0000000200000002 \\ \cdots \\ 0000000000002002\end{array}\right)$
where $a=0$ or 2 . The minimum Hamming weight of this code is 2. If $a=0$, the corresponding code $C^{(2)}$ has minimum Euclidean weight 4 , and if $a=2$, the code $C^{(3)}$ has $d_{E}=8$.
3) $k_{1} \geq 4$. Up to equivalence, the code $4 d_{4}$ with a generator matrix

$$
G_{1}=\left(\begin{array}{l}
1111000000000000 \\
0000111100000000 \\
0000000011110000 \\
0000000000001111
\end{array}\right)
$$

is the unique binary $\left[16, k_{1} \geq 4,4\right]$ code which satisfies the conditions of Theorem 2.1. In this case, $C_{1}$ is equivalent to the code with a generator matrix in the form (this form is more convenient for us)

$$
\left(\begin{array}{l}
1000110000001000 \\
0100001100000100 \\
0010000011000010 \\
0001000000110001
\end{array}\right)
$$

and then $C_{2}$ will be the code with a generator matrix
$\left(\begin{array}{l}1000110000001000 \\ 0100001100000100 \\ 0010000011000010 \\ 0001000000110001 \\ 0000100000001000 \\ 0000010000001000 \\ 0000001000000100 \\ 0000000100000100 \\ 0000000010000010 \\ 0000000001000010 \\ 0000000000100001 \\ 0000000000010001\end{array}\right)$.

TABLE II
swe Coefficients for the Type IV-I Codes of Length 16 (Partial)

|  | $b^{4}$ | $b^{5}$ | $b^{12}$ | $c^{2}$ | $c^{4}$ | $b^{4} c^{2}$ | $b^{8} c^{2}$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $C^{(1)}$ | 8 | 0 | 2048 | 72 | 892 | 528 | 0 |
| $C^{(2)}$ | 16 | 192 | 2048 | 40 | 444 | 544 | 3328 |
| $C^{(3)}$ | 0 | 64 | 2048 | 40 | 444 | 512 | 3840 |
| $C^{(4)}$ | 32 | 384 | 2048 | 24 | 220 | 576 | 4608 |
| $C^{(5)}$ | 8 | 192 | 2048 | 24 | 220 | 528 | 5376 |
| $C^{(6)}$ | 0 | 128 | 2048 | 24 | 220 | 512 | 5632 |

Since the interchanging the two elements 1 and 3 of certain coordinates gives equivalent codes, we can take the diagonal elements of $B$ to be 0 's. So, up to equivalence, we have the following possibilities for the matrix $B$ :

$$
\left(\begin{array}{l}
0000 \\
0000 \\
0000 \\
0000
\end{array}\right) \quad \text { or } \quad\left(\begin{array}{l}
0110 \\
1010 \\
1100 \\
0000
\end{array}\right) \quad \text { or } \quad\left(\begin{array}{l}
0110 \\
1001 \\
1001 \\
0110
\end{array}\right) .
$$

We denote the corresponding codes by $C^{(4)}, C^{(5)}$, and $C^{(6)}$.
Remark: Obviously, if we take for the matrix $B$

$$
\begin{array}{rr}
\left(\begin{array}{l}
0000 \\
0011 \\
0101 \\
0110
\end{array}\right) \text { or }\left(\begin{array}{l}
0101 \\
1010 \\
0101 \\
0010
\end{array}\right) \text { or }\left(\begin{array}{l}
0101 \\
1001 \\
0000 \\
1100
\end{array}\right) \\
\text { or }\left(\begin{array}{l}
0011 \\
0000 \\
1001 \\
1010
\end{array}\right) \text { or }\left(\begin{array}{l}
0011 \\
0011 \\
1100 \\
1100
\end{array}\right)
\end{array}
$$

we obtain codes equivalent to $C^{(4)}, C^{(5)}$, or $C^{(6)}$.
In Table II, we give some of the coefficients of the symmetrized weight enumerators of these six codes.
The six codes have different enumerators, so they are inequivalent.
Theorem 5.1: There are exactly six inequivalent Type IV-I codes of length 16.

In all cases, the minimum Hamming weight of $C$ is 2 . The codes $C^{(3)}$ and $C^{(6)}$ have minimum Euclidean weight 8 . So we proved the following theorem.
Theorem 5.2: For Type IV-I codes, $d_{H}(16)=2$ and $d_{E}(16)=8$.
Remark: An independent classification of the Type IV codes over $Z_{4}$ of length 16 has been done by Harada and Munemasa (see [10]). They have used the classification of the doubly even self-dual binary codes of length 32 [3].

## VI. Optimal Type IV Codes of Length 24

Proposition 6.1: If $C$ is Type IV code of length 24 then the minimum distance $d_{2}$ of its torsion code is 2 .

Proof: Suppose that $d_{2} \geq 4$. According to Proposition 4.1, the residue code $C_{1}$ should be a doubly even self-orthogonal $\left[24, k_{1}, d_{1} \geq\right.$ 8] code whose dual code $C_{2}$ has parameters [24, 24- $\left.k_{1}, d_{2} \geq 4\right]$. Using Brouwer's table [1] and Corollary 4.2, we have $6 \leq k_{1} \leq 11$
and $d_{1}=8$. Up to equivalence, $v=(1111111100 \cdots 0) \in C_{1}$. We can take a generator matrix of $C_{1}$ in the following form:

$$
G_{1}=\left(\begin{array}{cc}
11111111 & 00 \cdots 00 \\
O & D \\
E & F
\end{array}\right)
$$

where the matrix ( $O D$ ) generates the subcode of $C_{1}$ of all codewords with 0 's in the first eight coordinates. So $D$ generates a self-orthogonal $[16, s, \geq 8]$ code, and, therefore, $s \leq 5$ (see [5]). The matrix $E$ with the all-ones vector of length 8 generates the code $C_{E}$ with parameters [ $\left.8, k_{1}-s, 4\right]$. If $x \in C_{E}^{\perp}$ then $(x, 0) \in C_{1}^{\perp}=C_{2}$. Hence, the dual distance of $C_{E}$ is at least 4 and so it is equivalent to the extended Hamming code. It follows that $k_{1}-s=4$ and, therefore, $k_{1} \leq 9$ and $s \geq 2$. Hence,

$$
G_{1}=\left(\begin{array}{ccc}
11111111 & 00000000 & 00000000 \\
00000000 & 11111111 & 00000000 \\
00000000 & 00000000 & 11111111 \\
00000000 & v_{3} & w_{3} \\
& \cdots & \\
00000000 & v_{s} & w_{s} \\
11110000 & x_{1} & y_{1} \\
11001100 & x_{2} & y_{2} \\
10101010 & x_{3} & y_{3}
\end{array}\right)
$$

The vectors
$\mathbf{1}, v_{3}, \ldots, v_{s}, x_{1}, x_{2}, x_{3}$ and $\mathbf{1}, w_{3}, \ldots, w_{s}, y_{1}, y_{2}, y_{3}$
generate $[8,4,4]$ codes. We consider the following three cases.

1) $s=2$. Up to equivalence, $C_{1}$ has a generator matrix of type

$$
\left(\begin{array}{lll}
11111111 & 00000000 & 00000000 \\
00000000 & 1111111 & 00000000 \\
00000000 & 00000000 & 11111111 \\
11110000 & 11110000 & 11110000 \\
11001100 & 11001100 & 11001100 \\
10101010 & 10101010 & 10101010
\end{array}\right) .
$$

The Hadamard product of the last two rows has weight 6 which contradicts Theorem 2.1.
2) $s=3$. Then the vectors $11111111,11110000, y_{1}, y_{2}, y_{3}$ are linearly dependent, so up to equivalence, $y_{1}=0$. Hence $C_{1}$ has a generator matrix of type
$\left(\begin{array}{lll}11111111 & 00000000 & 00000000 \\ 00000000 & 11111111 & 00000000 \\ 00000000 & 00000000 & 1111111 \\ 00000000 & 11110000 & 11110000 \\ 11110000 & 11110000 & 00000000 \\ 11001100 & 11001100 & 11001100 \\ 10101010 & 10101010 & 10101010\end{array}\right)$.

The Hadamard product of the last two rows has weight 6 which contradicts Theorem 2.1.
3) $s \geq 4$. Up to equivalence,
$v_{3}=w_{3}=(11110000)$ and $v_{4}=w_{4}=(11001100)$.

The vectors (11111111), (11110000), (11001100), $y_{1}, y_{2}, y_{3}$ are linearly dependent and so we can take $y_{1}=0$. According to Theorem 2.1,
$w_{H}\left(\left(0, v_{i}, w_{i}\right) *\left(11110000, x_{1}, 00000000\right)\right)=w_{H}\left(v_{i} * x_{1}\right)=4$
for $i=3,4$, which is impossible.
Corollary 6.2: $\quad d_{L}(24)=4, d_{H}(24)=2$, and $d_{E}(24)=8$.
Proof: The vector $x \in C_{2}$ of weight 2 has Lee weight 4, Hamming weight 2 , and Euclidean weight 8 . Hence, $d_{L}(C) \leq 4, d_{H}(C) \leq$ 2 , and $d_{E}(C) \leq 8$ for any Type IV $Z_{4}$-code $C$ of length 24 . It follows that $d_{L}(C)=4$ and $d_{H}(C)=2$. The code $K_{12} \oplus K_{12}$ (see [5]) has minimum Euclidean weight 8 and, therefore, $d_{E}(24)=8$.

## Acknowledgment

The author wishes to thank Prof. J. Simonis for his helpful advices and recommendations. The author is grateful to the Delft University of Technology for the excellent working conditions provided.

## References

[1] A. E. Brouwer, "Bounds on the size of linear codes," in Handbook of Coding Theory, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998.
[2] S. Buyuklieva, "On the binary self-dual codes with an automorphism of order 2," Des. Codes Cryptogr., vol. 12, pp. 39-48, 1997.
[3] J. H. Conway, V. Pless, and N. J. A. Sloane, "The binary self-dual codes of length up to 32: A revised enumeration," J. Combin. Theory Ser. A, vol. 60, pp. 183-195, 1992.
[4] J. H. Conway and N. J. A. Sloane, "Self-dual codes over the integers modulo 4," J. Combin. Theory Ser. A, vol. 62, pp. 30-45, 1993.
[5] S. Dougherty, P. Gaborit, M. Harada, A. Munemasa, and P. Solé, "Type IV self-dual codes over rings," IEEE Trans. Inform. Theory, vol. 45, pp. 2345-2360, Nov. 1999.
[6] S. B. Encheva and H. E. Jensen, "Optimal binary linear codes and $Z_{4}$-linearity," IEEE Trans. Inform. Theory, vol. 42, pp. 1216-1222, July 1996.
[7] J. Fields and P. Gaborit, "On the non $Z_{4}$-linearity of certain good binary codes," IEEE Trans. Inform. Theory, vol. 45, pp. 1674-1677, July 1999.
[8] J. H. Griesmer, "A bound for error-correcting codes," IBM J. Res. Develop., vol. 4, pp. 532-542, 1960.
[9] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $Z_{4}$-linearity of Kerdock, Preparata, Goethals and related codes," IEEE Trans. Inform. Theory, vol. 40, pp. 301-319, Mar. 1994.
[10] M. Harada and A. Munemasa, "Classification of type IV self-dual $Z_{4}$-codes of length 16," Finite Fields Their Appl., vol. 6, pp. 244-254, 2000.
[11] C. L. Mallows and N. J. A. Sloane, "An upper bound for self-dual codes," Inform. Contr., vol. 22, pp. 188-200, 1973.
[12] V. Pless, J. S. Leon, and J. Fields, "All $Z_{4}$ codes of type II and length 16 are known," J. Combin. Theory Ser. A, vol. 78, pp. 32-50, 1997.
[13] E. Rains, "Optimal self-dual codes over $Z_{4}$," Discr. Math., vol. 203, pp. 215-228, 1999.


[^0]:    Manuscript received April 5, 2000; revised April 5, 2001
    The author was with the Department of Mediamatics, Faculty of Information Technology and Systems, Delft University of Technology, Delft, The Netherlands. She is now with the Department of Mathematics and Informatics, University of Veliko Tarnovo, 5000 Veliko Tarnovo, Bulgaria (e-mail: stefkailiya@yahoo.com)

    Communicated by P. Solé, Associate Editor for Coding Theory.
    Publisher Item Identifier S 0018-9448(02)01064-7.

