Some Results on Type IV Codes Over Z_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 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 Z_4 -code of length 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 $n \ge 24$, $n \neq 32$ 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, 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 $n \ge 24$, $n \ne 32$, 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

$$d_L \le 4\left(1 + \left\lfloor \frac{n}{12} \right\rfloor\right).$$

We prove that no Type IV self-dual Z_4 -code of length $n \ge 12$, $n \ne 16$, 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 $n \ge 12$, $n \ne 16$, and minimum Lee weight d_L then

$$d_L \le 4 \left\lfloor \frac{n}{12} \right\rfloor.$$

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

$$d_H = \frac{1}{2} d_L \qquad d_E \le 2 d_L.$$

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.

A Type IV-I (resp., Type IV-II) code C is *Lee-optimal*, *Euclidean-optimal*, 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 $n \ge 24$, $n \ne 32$ 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 Euclidean weight of a codeword is the rational sum of the Euclidean weights of its components. The sual 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

$$\begin{pmatrix} I_{k_1} & A & B_1 + 2B_2 \\ O & 2I_{k_2} & 2D \end{pmatrix}$$
(1)

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 $[n, k_1]$ code C_1 with generator matrix

$$\begin{pmatrix} I_{k_1} & A & B_1 \end{pmatrix} \tag{2}$$

is called the *residue code* of C. The binary $[n, k_1 + k_2]$ code C_2 with generator matrix

$$\begin{pmatrix} I_{k_1} & A & B_1 \\ O & I_{k_2} & D \end{pmatrix}$$
(3)

TABLE I The Highest Minimum Weights for Type IV-I \mathbb{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	$\mathcal{D}_4^\oplus[5]$
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

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 \mathbb{Z}_4^n by

$$x \cdot y = x_1 y_1 + \dots + x_n y_n \pmod{4}.$$

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

$$C^{\perp} = \{ x \in Z_4^n | x \cdot y = 0 \ \forall y \in C \}.$$

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

$$\begin{pmatrix} I_{k_1} + 2B & A & B_1 \\ O & 2I_{k_2} & 2D \end{pmatrix}$$
(4)

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

$$w_H(x*y) \equiv 0 \pmod{4}$$

for any x and $y \in C_1$,

3) the number of 2's in each row of $I_{k_1} + 2B$ 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 ϕ is a distance-preserving map from Z_4^n (Lee distance) to Z_2^{2n} (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 β and γ 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 $\phi: Z_4^n \to Z_2^{2n}$ is given by

$$\phi(c) = (\beta(c), \gamma(c)), \qquad c \in Z_4^n.$$

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 $w_H(u_i) < 2d_2, i = 1, \ldots, t$, 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 C be an extremal binary doubly even self-dual code of length 2n which is the Gray image of a linear Z_4 -code C. Since $\phi(-c) = (\gamma(c), \beta(c))$, it follows that C is fixed under the "swap" map σ that interchanges the left and right halves of each codeword. In other words

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

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}_{σ} , we denote the fixed subcode of \mathcal{C} under σ , namely, $\mathcal{C}_{\sigma} = \{v \in \mathcal{C}: \sigma(v) = v\}$. Obviously, $v \in \mathcal{C}_{\sigma}$ iff vis a codeword in \mathcal{C} and $v = (v_1, v_2, \ldots, v_n, v_1, v_2, \ldots, v_n)$. If π is the map from \mathcal{C}_{σ} to Z_2^n defined by $\pi(v) = (v_1, v_2, \ldots, v_n)$, then $C_2 = \pi(\mathcal{C}_{\sigma})$. For the code C_1 we have $C_1 = \psi(\mathcal{C})$ where $\psi: Z_2^{2n} \to Z_2^n$ is defined by

$$\psi(v) = (v_1 + v_{n+1}, v_2 + v_{n+2}, \dots, v_n + v_{2n}).$$

Theorem 3.1 [2]: If C is a binary self-dual code of length 2n with an automorphism σ of order 2 without fixed points then C_1 is a self-orthogonal code of length n and C_2 is its dual code.

Corollary 3.2: If C is a binary doubly even self-dual code of length 2n with an automorphism σ of order 2 without fixed points then C_1 contains the all-ones vector.

Proof: Since all weights in C_{σ} are divisible by four, all weights in C_2 are even and so $\mathbf{1} \in C_1 = C_2^{\perp}$.

Let n = 12m + 4r, r = 0, 1, 2, and let the minimum distance of C be 4m + 4. Then the minimum distance of C_2 has to be at least 2m + 2.

Corollary 3.3: If C is an extremal doubly even self-dual code of length $2n = 24m + 8r \ge 24$ which is Z_4 -linear, then the minimum distance of C_1 is at least 4m + 4.

Proof: Let $u_1, u_2, \ldots, u_t \in C_1$ be the codewords for which $w_H(u_i) < 4m+4, i=1, \ldots, t$. If $t \ge 1$, without loss of generality, we can take $u_1 = (1 \cdots 10 \cdots 0)$ with $4m+4 > w_H(u_1) \ge 2m+2 \ge 4$. According to Theorem 2.3, the code C_1 has a generator matrix with first row u_1 of the form

$$G_1 = \begin{pmatrix} 11 \cdots 11 & 00 \cdots 00 \\ 0 & G_1' \end{pmatrix}$$

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 4m + 4.

Theorem 3.4: The extremal doubly even self-dual codes of length $n \ge 24$, $n \ne 32$, are not Z_4 -linear.

Proof: Let C be a Z_4 -linear doubly even self-dual binary code of length 24m+8r, $r \in \{0, 1, 2\}$, $m \ge 1$, and minimum weight d = 4m+4. Then, C_1 is a self-orthogonal $[12m+4r, s, d_1 \ge 4m+4]$, and its dual code C_2 has length 12m+4r, dimension $12m+4r-s \ge 6m+2r$, and minimum distance at least 2m+2. Using the Griesmer bound [2], we have

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

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

$$A \ge \sum_{i=1}^{l} \left| \frac{2^{l}+1}{2^{i}} \right| = \sum_{i=1}^{l} \left| 2^{l-i} + \frac{1}{2^{i}} \right|$$
$$= \sum_{i=1}^{l} (2^{l-i}+1) = 2^{l} - 1 + l \Rightarrow A - l \ge 2^{l} - 1$$

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

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

Let $x, y \in C_1$ and x * y = 0. Then

$$w_H(\mathbf{1} + x + y) = 12m + 4r - w_H(x) - w_H(y)$$

$$\leq 12m + 4r - 2(4m + 4) = 4m + 4r - 8 \leq 4m$$

and so y = 1 + x. Hence, C_1 has a generator matrix of the form

$$G_1 = \begin{pmatrix} 00 \cdots 00 & 11 \cdots 11 \\ 11 \cdots 11 & 00 \cdots 00 \\ x_3 & y_3 \\ \cdots & \cdots \\ x_s & y_s \end{pmatrix}$$

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 6m + 2r. According to Theorem 2.2

$$(x_i, y_i) * (1, 0) = (x_i, 0) \in C_1, \qquad i = 3, \dots, s.$$

It follows that the vectors $(1, 0), (x_3, 0), \ldots, (x_s, 0)$ generate a subcode of C_2 with dimension s-1 and minimum distance at least 2m+2. Hence the vectors $1, x_3, \ldots, x_s$ generate a $[d_1, s-1, \ge 2m+2]$ code. Using the Griesmer bound, we have

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

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

$$d_1 \ge 3m + 3 + A + s - 3 - l$$

$$\ge 3m + A - l + 3m + 1 + A - l = 6m + 1 + 2(A - l).$$

We consider the following three cases.

)
$$l \ge 2$$
. Then
 $A - l \ge 2^{l} - 1 \ge 3 \Rightarrow d_1 \ge 6m + 7 > 6m + 2r;$

a contradiction

1

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

$$A - l = \left\lceil \frac{m+1}{2} \right\rceil - 1 = 1 \Rightarrow d_1 \ge 6m + 3.$$

If r = 0 or 1, we have $d_1 > 6m + 2r$. Let r = 2. Then C_1 must be a $[12m + 8, s \ge 3m + 2, 6m + 4]$ 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 $[44, s \ge 11, 22]$ code, which is impossible.

3) l = 0. In this case, $2 \ge m + 1 > 1$ and m = 1. It follows that A - l = 0 and $d_1 \ge 6m + 1 = 7$, but d_1 is even and so d_1 is at least 8. If r = 0, we have $d_1 > 6m$, which is a contradiction. When r = 2, C_2 should be a $[20, 20 - s, \ge 4]$ code and hence $s \ge 6$ [1]. It follows that C_1 is a $[20, s \ge 6, d_1 = 8 \text{ or } 10]$ 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 $[d_1 = 8, s - 1 \ge 5, \ge 4]$ code. But codes with these parameters do not exist.

In the case r = 1, 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 $2e_8$. 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 $n = 12m + 4r, r \in \{0, 1, 2\}, m > 0$, and minimum Lee weight

 $d_L = 4m + 4$. Then its Gray image $C = \phi(C)$ is a binary doubly even self-dual [24m + 8r, 12m + 4r, 4m + 4] code. We proved that these codes are not Z_4 -linear for $m \ge 2$ and for m = 1, r = 0, 2. Hence, no Type IV Z_4 -code of length $n \ge 12, n \ne 16$, 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 $2d_2$.

Proof: Obviously, the minimum distance of C_1 is at least 4. This proves the proposition in the case when $d_2 = 2$.

Let $d_2 \ge 4$ and let $u_1, u_2, \ldots, u_t \in C_1$ be the codewords for which $w_H(u_i) < 2d_2, i = 1, \ldots, t$. If $t \ge 1$, without loss of generality, we can take $u_1 = (1 \cdots 10 \cdots 0)$ with $w_H(u_1) \ge d_2 \ge 4$. According to Theorem 2.3, the code C_1 has a generator matrix with first row u_1 of the form

$$G_1 = \begin{pmatrix} 11 \cdots 11 & 00 \cdots 00 \\ 0 & G_1' \end{pmatrix}$$

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 $2d_2$.

Corollary 4.2: There is no Type IV code of type $4^{\frac{n}{2}}$.

Proof: Let C be Type IV code of type $4^{\frac{n}{2}}$. 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 $d_2 = d_1 \ge 2d_2$ which is impossible.

Proposition 4.3: If C is Type IV code and the minimum distance of its torsion code is d_2 , then $d_L(C) = 2d_2$, $d_H(C) = d_2 = \frac{1}{2} d_L(C)$, $d_E(C) \le 4d_2$.

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 2y is a codeword in C of Hamming weight d_2 , Lee weight $2d_2$, and Euclidean weight $4d_2$. Hence, the minimum Hamming, Lee, and Euclidean weights of this code are at most d_2 , $2d_2$, and $4d_2$, 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 $x \in 2C_2$ and $w_H(x) \ge d_2$, $w_L(x) = 2w_H(x) \ge 2d_2$.

Now let $n_1(x) + n_3(x) \ge 1$. In this case, $x = x_1 + x_2$ where $x_1 \ne 0$ 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 $2C_2$. Then

$$x_1 = v_{i_1} + \dots + v_{i_{s_1}} + 3v_{j_1} + \dots + 3v_{j_{s_2}}$$

where $\{i_1, \ldots, i_{s_1}\} \cap \{j_1, \ldots, j_{s_2}\} = \emptyset$ and

{

$$i_1, \ldots, i_{s_1} \} \cup \{ j_1, \ldots, j_{s_2} \} \subset \{ 1, \ldots, k_1 \}.$$

It follows that $n_1(x) + n_3(x) = n_1(x_1) + n_3(x_1)$. But the number of 1's and 3's in this vector is equal to the number of 1's in the binary vector $x'_1 = v'_{i_1} + \cdots + v'_{i_{s_1}} + v'_{j_1} + \cdots + v'_{j_{s_2}}$, where v'_i is the *i*th row of the matrix (2). Since x'_1 is a nonzero codeword in C_1 , its weight

$$w_H(x) \ge n_1(x) + n_3(x) = n_1(x_1) + n_3(x_1) \ge d_1 \ge 2d_2$$

$$w_L(x) \ge w_H(x) \ge 2d_2.$$

is at least d_1 . Hence, $n_1(x_1) + n_3(x_1) \ge d_1$ and

So we proved that minimum Lee weight of C is exactly $2d_2$. \Box

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 $n \ge 12$, $n \ne 16$ then

$$d_H(C) \le 2\lfloor n/12 \rfloor$$

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_f5 . 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 $w_H(x * y) \equiv 0 \pmod{4}$ 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 = (111100000000000). Then C_1 has a generator matrix of the form

$$G_1 = \begin{pmatrix} 1111 & 00\cdots 00\\ 0000 & G_1' \end{pmatrix}$$

where G'_1 generates a doubly even binary $[12, k_1 - 1, \ge 4]$ code. We consider three cases.

1)
$$k_1 = 2$$
. Then

$$G_1 = \begin{pmatrix} 111100000000000\\ 00001111111111 \end{pmatrix}$$

and since C_1 satisfies the conditions of Theorem 2.1, the code C with a generator matrix

[]	111100000000000000\
(000011111111111
6	22000000000000000
1	20200000000000000
(0000220000000000000000000000000000000
(00002020000000000
١ (00002000000000020/

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 = (000011110000000). Then

and C is equivalent to a code with generator matrix

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) $k_1 \ge 4$. Up to equivalence, the code $4d_4$ with a generator matrix

is the unique binary $[16, k_1 \ge 4, 4]$ 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)

1	/1000110000001000\
ĺ	0100001100000100
l	0010000011000010
١	0001000000110001

and then C_2 will be the code with a generator matrix

/1000110000001000
0100001100000100
0010000011000010
0001000000110001
000010000001000
000001000001000
000000100000100
000000010000100
0000000010000010
0000000001000010
0000000000100001
\0000000000010001/

 $\begin{array}{c} \mbox{TABLE} \quad \mbox{II} \\ \mbox{swe Coefficients for the Type IV-I Codes of Length 16 (Partial)} \end{array}$

	24	6 ⁶	612	c^2	c4	$b^{4}c^{2}$	$b^{8}c^{2}$
$C^{(1)}$	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:

(0000)		/0110		/0110	
0000	or	1010	or	1001	
0000		1100		1001	
\0000/		\0000 <i>]</i>		\0110 <i>]</i>	

We denote the corresponding codes by $C^{(4)}$, $C^{(5)}$, and $C^{(6)}$.

Remark: Obviously, if we take for the matrix B

$$\begin{pmatrix} 0000\\ 0011\\ 0101\\ 0110 \end{pmatrix} \text{ or } \begin{pmatrix} 0101\\ 1010\\ 0010 \end{pmatrix} \text{ or } \begin{pmatrix} 0101\\ 1001\\ 0000\\ 1100 \end{pmatrix}$$
$$\text{ or } \begin{pmatrix} 0011\\ 0000\\ 1001\\ 1000 \end{pmatrix} \text{ or } \begin{pmatrix} 0011\\ 0011\\ 1100\\ 1000 \end{pmatrix}$$

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 $d_2 \ge 4$. According to Proposition 4.1, the residue code C_1 should be a doubly even self-orthogonal [24, k_1 , $d_1 \ge 8$] code whose dual code C_2 has parameters [24, 24 - k_1 , $d_2 \ge 4$]. Using Brouwer's table [1] and Corollary 4.2, we have $6 \le k_1 \le 11$

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:

$$G_1 = \begin{pmatrix} 11111111 & 00 \cdots 00 \\ O & D \\ E & F \end{pmatrix}$$

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 [8, $k_1 - s$, 4]. 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,

	/11111111	00000000	00000000
	00000000	11111111	00000000
	00000000	00000000	11111111
	00000000	v_3	w_3
$G_1 =$			
	00000000	v_s	w_s
	11110000	x_1	y_1
	11001100	x_2	y_2
	10101010	x_3	y_3

The vectors

1, $v_3, \ldots, v_s, x_1, x_2, x_3$ and **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

/11111111	00000000	00000000	
00000000	11111111	00000000	
00000000	00000000	11111111	
11110000	11110000	11110000	•
11001100	11001100	11001100	
\10101010	10101010	10101010/	

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

/ 11111111	00000000	00000000
00000000	11111111	00000000
00000000	00000000	11111111
00000000	11110000	11110000
11110000	11110000	00000000
11001100	11001100	11001100
10101010	10101010	10101010/

The Hadamard product of the last two rows has weight 6 which contradicts Theorem 2.1.

3) $s \ge 4$. 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,

$$w_H((0, v_i, w_i) * (11110000, x_1, 0000000)) = w_H(v_i * x_1) = 4$$

for
$$i = 3, 4$$
, which is impossible.

Corollary 6.2: $d_L(24) = 4$, $d_H(24) = 2$, 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

- 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 Z₄-linearity," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1216–1222, July 1996.
- [7] J. Fields and P. Gaborit, "On the non Z₄-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 Z₄-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 Z₄-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 Z₄ 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 Z₄," *Discr. Math.*, vol. 203, pp. 215–228, 1999.