Optimal Self-Dual Codes over $\mathbb{F}_2 + v\mathbb{F}_2$

Koichi Betsumiya
Graduate School of Mathematics
Nagoya University
Nagoya 464–8602, Japan
and
Masaaki Harada
Department of Mathematical Sciences
Yamagata University
Yamagata 990–8560, Japan

October 19, 2000

Abstract

In this correspondence, we study optimal self-dual codes and Type IV self-dual codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$ of order 4. We give improved upper bounds on minimum Hamming and Lee weights for such codes. Using the bounds, we determine the highest minimum Hamming and Lee weights for such codes of lengths up to 30. We also construct optimal self-dual codes and Type IV self-dual codes.

Index Terms: Self-dual codes over rings, Type IV self-dual codes and binary optimal codes.

1 Introduction

There are four different rings of order 4, namely the finite field $\mathbb{F}_4$, the ring $\mathbb{Z}_4$ of integers modulo 4 and two other rings denoted by $\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1+u\}$ with $u^2 = 0$ and $\mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, 1+v\}$ with $v^2 = v$. Self-dual codes over $\mathbb{F}_4$ are covered by the classical coding theory. Recently self-dual codes over $\mathbb{Z}_4$ and $\mathbb{F}_2 + u\mathbb{F}_2$ have been widely studied.

In this correspondence, we study optimal self-dual codes and Type IV self-dual codes over $\mathbb{F}_2 + v\mathbb{F}_2$ with respect to the Hermitian and Euclidian inner products. Bachoc [1] studies Hermitian self-dual codes over $\mathbb{F}_2 + v\mathbb{F}_2$. Upper bounds on the Bachoc minimum weights of Hermitian self-dual codes are given in [1] and optimal Hermitian self-dual codes with

respect to the weight are constructed. In this correspondence, we investigate the minimum Hamming weights and the minimum Lee weights. In [7] and [6], upper bounds on minimum Hamming and Lee weights of Hermitian self-dual codes and Hermitian Type IV self-dual codes of lengths up to 24, are given, respectively. In Section 3, we show that the minimum Hamming weight of a code over $\mathbb{F}_2 + v\mathbb{F}_2$ is the same as the minimum Lee weight. Using some characterization of Hermitian self-dual codes over $\mathbb{F}_2 + v\mathbb{F}_2$, we give improved upper bounds on minimum Hamming and Lee weights for Hermitian self-dual codes and Hermitian Type IV self-dual codes and we construct optimal Hermitian self-dual codes and Hermitian Type IV self-dual codes in Section 4. In Section 5, we investigate optimal Euclidean self-dual codes.

2 Self-Dual Codes over $\mathbb{F}_2 + v\mathbb{F}_2$

A code C of length n over $\mathbb{F}_2+v\mathbb{F}_2$ is an $(\mathbb{F}_2+v\mathbb{F}_2)$-submodule of $(\mathbb{F}_2+v\mathbb{F}_2)^n$ where $\mathbb{F}_2+v\mathbb{F}_2$ is a commutative ring $\{0, 1, v, 1+v\}$ with $v^2 = v$. An element of C is called a codeword of C. A generator matrix of C is a matrix whose rows generate C. Three different weights for codes over $\mathbb{F}_2 + v\mathbb{F}_2$ are known, namely the Hamming, Lee and Bachoc weights [1], [6] and [7]. The Hamming weight of a codeword is the number of non-zero components. The Lee weights of the elements $0, 1, v$ and $1+v$ are $0, 2, 1$ and 1, respectively. The Bachoc weight is defined in [1] and the weights of the elements $0, 1, v$ and $1+v$ are $0, 1, 2$ and 2, respectively. The Lee and Bachoc weights of a codeword are the rational sums of the Lee and Bachoc weights of its components, respectively. The minimum Hamming, Lee and Bachoc weights, d_H, d_L and d_B of C are the smallest Hamming, Lee and Bachoc weights among all non-zero codewords of C, respectively.

We define two inner products (x, y) and $[x, y]$ of x and y in $(\mathbb{F}_2 + v\mathbb{F}_2)^n$ where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are two elements of $(\mathbb{F}_2 + v\mathbb{F}_2)^n$. The Euclidean inner product is defined as $(x, y) = x_1y_1 + \cdots + x_ny_n$, and the Hermitian inner product is defined as $[x, y] = x_1\overline{y_1} + \cdots + x_n\overline{y_n}$, where $\overline{0} = 0$, $\overline{1} = 1$, $\overline{v} = v+1$ and $\overline{v+1} = v$. The dual code $C^\perp$ with respect to the Euclidean inner product of C is defined as $C^\perp = \{x \in (\mathbb{F}_2+v\mathbb{F}_2)^n |\ (x, y) = 0 \text{ for all } y \in C\}$ and the dual code C^* with respect to the Hermitian inner product of C is defined as $C^* = \{x \in (\mathbb{F}_2 + v\mathbb{F}_2)^n |\ [x, y] = 0 \text{ for all } y \in C\}$. C is *Euclidean self-dual* if $C = C^\perp$ and C is *Hermitian self-dual* if $C = C^*$. Recently Type IV self-dual codes over rings of order 4 are defined in [6]. A self-dual code is *Type IV* if all the Hamming weights are even.

3 Minimum Weights

In this section, we give a characterization of minimum Hamming and Lee weights. We first study self-dual codes over $\mathbb{F}_2 + v\mathbb{F}_2$ using the Chinese remainder theorem.

Define the map

$$\Phi : \mathbb{F}_2 + v\mathbb{F}_2 \to \mathbb{F}_2 \times \mathbb{F}_2,$$

where $\Phi(0) = (0,0)$, $\Phi(1) = (1,1)$, $\Phi(v) = (0,1)$ and $\Phi(1+v) = (1,0)$. Φ is a ring-isomorphism by the Chinese remainder theorem. The map is extended to $(\mathbb{F}_2 + v\mathbb{F}_2)^n$ naturally. Let C be a code over $\mathbb{F}_2 + v\mathbb{F}_2$, then there are binary codes C_1 and C_2 such that $C = \Phi^{-1}(C_1, C_2)$ and we denote C by $CRT(C_1, C_2)$. Note that C_1 and C_2 are uniquely determined for each $CRT(C_1, C_2)$. Using the above map, characterizations of self-dual codes and Type IV self-dual codes over $\mathbb{F}_2 + v\mathbb{F}_2$ are given.

Lemma 1 ([5] and [6]) *$CRT(C_1, C_2)$ is a Euclidean self-dual code if and only if C_1 and C_2 are binary self-dual codes. $CRT(C_1, C_2)$ is Euclidean Type IV self-dual if and only if $C_1 = C_2$.*

Lemma 2 ([1] and [6]) *$CRT(C_1, C_2)$ is a Hermitian self-dual code if and only if $C_2 = C_1^{\perp}$. $CRT(C_1, C_1^{\perp})$ is Hermitian Type IV self-dual if and only if C_1 and $C_1^{\perp}$ are even codes.*

Let c be a codeword of $C = CRT(C_1, C_2)$ then c can be uniquely written as $c = \Phi^{-1}(c_1, c_2)$ where c_1 and c_2 are codewords of C_1 and C_2, respectively. Let $w_H(c)$ and $w_L(c)$ be the Hamming and Lee weights of c, respectively. Then

$$(1) \qquad \begin{aligned} w_H(c) &= w_H(c_1) + w_H(c_2) - w_H(c_1 * c_2), \\ w_L(c) &= w_H(c_1) + w_H(c_2), \end{aligned}$$

where $c_1 * c_2$ denotes the Hadamard product of c_1 and c_2.

Proposition 3 *Let d_H and d_L be the minimum Hamming and Lee weights of $CRT(C_1, C_2)$, respectively. Then*

$$d_H = d_L = \min\{d(C_1), d(C_2)\},$$

where $d(C_i)$ denotes the minimum weight of a binary code C_i.

Proof. The two cases are similar, thus we show that $d_H = \min\{d(C_1), d(C_2)\}$. Let c be a codeword of $CRT(C_1, C_2)$ then $c = \Phi^{-1}(c_1, c_2)$ where c_1 and c_2 are codewords of C_1 and C_2, respectively. Then it follows from (1) that $w_H(c) \geq \max\{w_H(c_1), w_H(c_2)\}$. Thus $d_H \geq \min\{d(C_1), d(C_2)\}$. Assume that $d(C_1) \geq d(C_2)$. Let c_2' be a codeword with weight $d(C_2)$ in C_2 then $\Phi^{-1}(0, c_2')$ is a codeword of Hamming weight $d(C_2)$. The result follows. □

By the above proposition, it is sufficient to consider only minimum Hamming weights. Thus the minimum Hamming weight is shortly said to be the minimum weight from now on. We say that a self-dual (resp. Type IV self-dual) code C is *optimal* if C has the highest minimum weight among all self-dual (resp. Type IV self-dual) codes of that length.

4 Optimal Hermitian Self-Dual Codes

In [7], weak upper bounds on minimum weights of Hermitian self-dual codes of lengths up to 24 are given. In this section, we determine the exact highest minimum weight of such codes for length up to 30.

First we give improved upper bounds on minimum weights using the characterization of Hermitian self-dual codes given in Section 3.

Proposition 4 *Let $d_{max}(n,k)$ be the highest minimum weight among all binary linear $[n,k]$ codes. The highest minimum weight $d_{SD}(n)$ among all Hermitian self-dual codes of length n is bounded by*

$$d_{SD}(n) \leq d_{max}\left(n, \lfloor (n+1)/2 \rfloor\right).$$

Proof. By Lemma 2 and Proposition 3, the minimum weight of a Hermitian self-dual code $CRT(C_1, C_1^{\perp})$ is $\min\{d(C_1), d(C_1^{\perp})\}$. Thus we have

$$d_{SD}(n) \leq \max_{1 \leq k \leq n-1} \min\{d_{max}(n,k), d_{max}(n,n-k)\}.$$

Since $d_{max}(n,k) \leq d_{max}(n,k-1)$, the result follows. □

Lower and upper bounds on minimum weights for binary linear codes are given in [3]. Thus one can easily obtain the highest possible minimum weights of Hermitian self-dual codes using the bounds.

Corollary 5 *Let $d'_{max}(n,k)$ be the highest minimum weight among all binary linear even $[n,k]$ codes whose dual codes are even. The highest minimum weight $d_{IV}(n)$ among all Hermitian Type IV self-dual codes of length n is bounded by*

$$d_{IV}(n) \leq d'_{max}(n, n/2).$$

Proof. Similar to that of Proposition 4. Note that a Hermitian Type IV self-dual code of length n exists if and only if n is even [6]. □

We determine the highest possible minimum weight of Hermitian Type IV self-dual codes using the following upper bound instead of Corollary 5 since $d'_{max}(n,k)$ is not known.

Corollary 6 $d_{IV}(n) \leq 2\left\lfloor \frac{d_{SD}(n)}{2} \right\rfloor$.

We now present methods to construct optimal Hermitian self-dual codes:

- **Method FSD**: Let B be a binary formally self-dual $[n, n/2, d]$ code. Note that $B^{\perp}$ is also an $[n, n/2, d]$ code. By Lemma 2 and Proposition 3, $CRT(B, B^{\perp})$ is a Hermitian self-dual code over $\mathbb{F}_2 + v\mathbb{F}_2$ with minimum weight d of length n. Moreover if B is even then $CRT(B, B^{\perp})$ is a Hermitian Type IV self-dual code.

- **Method SD**: Let B be a binary self-dual $[n, n/2, d]$ code. Since B and $B^{\perp}$ are even, $CRT(B, B^{\perp})$ is a Hermitian Type IV self-dual code with minimum weight d of length n by Lemma 2.

- **Method Type IV**: If the existence of a Hermitian Type IV self-dual code with minimum weight d of length n gives one of a Hermitian self-dual code with minimum weight d of this length. Thus Hermitian Type IV self-dual codes with high minimum weights given in Table 1 are used to determine the highest minimum weight of Hermitian self-dual codes (e.g., $n = 2, 4, 8$).

- **Method P**: Let B be a binary formally self-dual $[n, n/2, d]$ code. There is a coordinate of B such that the punctured code P obtained by deleting the coordinate is an $[n-1, n/2]$ code. Then it is easy to see that the dual code of P is an $[n-1, n/2-1]$ code with minimum weight $\geq d-1$. Hence $CRT(P, P^{\perp})$ is a Hermitian self-dual code of length $n-1$ with minimum weight d or $d-1$.

It is well known that there are binary self-dual codes with parameters $[2, 1, 2]$, $[4, 2, 2]$, $[6, 3, 2]$, $[8, 4, 4]$, $[10, 5, 4]$, $[16, 8, 4]$, $[22, 11, 6]$, $[24, 12, 8]$, $[26, 13, 6]$ and $[32, 16, 8]$ (cf. [4]). There are extremal formally self-dual even $[n, n/2, 2[n/8] + 2]$ codes of lengths $n = 12$, 14, 18, 20, 28 and 30 [9]. Thus Hermitian Type IV self-dual codes with the minimum weight meeting the upper bound given in Corollary 6 are constructed for length up to 32. We list in Table 1 the exact highest minimum weight $d_{IV}(n)$ of Hermitian Type IV self-dual codes of length $n \leq 32$.

Table 1: The highest minimum weight of Hermitian Type IV self-dual codes of length up to 32

Length n	$d_{IV}(n)$	Method	Length n	$d_{IV}(n)$	Method
2	2	SD	18	6	FSD
4	2	SD	20	6	FSD
6	2	SD	22	6	SD
8	4	SD	24	8	SD
10	4	SD	26	6	SD
12	4	FSD	28	8	FSD
14	4	FSD	30	8	FSD
16	4	SD	32	8	SD

Similarly to Hermitian Type IV self-dual codes, by the above methods, we construct optimal Hermitian self-dual codes with the minimum weight meeting the upper bound given in Proposition 4 for length $n \leq 32$ except $n = 11, 13, 31$. We list in Table 2 the exact highest minimum weight $d_{SD}(n)$ of Hermitian self-dual codes of length $n \leq 30$ and $n = 32$.

Recently a number of optimal binary odd formally self-dual codes have been construted in [2]. In particular, odd formally self-dual codes with parameters $[16, 8, 5]$, $[22, 11, 7]$ and $[26, 13, 7]$ are found. These codes have higher minimum weights than any even formally self-dual code of that length. QR_{17} is the binary quadratic residue $[17, 9, 5]$ code and G_{23} is the binary Golay $[23, 12, 7]$ code. The dual codes of QR_{17} and G_{23} have minimum weights 6 and 8, respectively. We have found by computer a linear $[11, 6, 4]$ code C_{11} with $d(C_{11}^{\perp}) = 4$ and a linear $[13, 7, 4]$ code C_{13} with $d(C_{13}^{\perp}) = 4$ with generator matrices

$$\begin{pmatrix} 100000 & 00111 \\ 010000 & 01011 \\ 001000 & 01101 \\ 000100 & 10011 \\ 000010 & 10101 \\ 000001 & 11001 \end{pmatrix} \text{ and } \begin{pmatrix} 1000000 & 000111 \\ 0100000 & 001011 \\ 0010000 & 001101 \\ 0001000 & 010011 \\ 0000100 & 100011 \\ 0000010 & 110001 \\ 0000001 & 111101 \end{pmatrix},$$

respectively. Hence Hermitian self-dual codes with minimum weight 4 are constructed from the above codes for lengths 11 and 13. For length 31, the binary quadratic residue code has parameters $[31, 16, 7]$ and its dual code has parameters $[31, 15, 8]$. Thus these codes correspond to a Hermitian self-dual code with minimum weight 7 of length 31. However we do not know if there is a Hermitian self-dual code with minimum weight 8.

Table 2: The highest minimum weight of Hermitian self-dual codes of length up to 32

Length n	$d_{SD}(n)$	Method	Length n	$d_{SD}(n)$	Method
1	1	P	17	5	P, QR_{17}
2	2	Type IV	18	6	Type IV
3	2	P	19	5	P
4	2	Type IV	20	6	Type IV
5	2	P	21	6	P
6	3	FSD	22	7	FSD
7	3	P	23	7	P, G_{23}
8	4	Type IV	24	8	Type IV
9	3	P	25	6	P
10	4	Type IV	26	7	FSD
11	4	C_{11}	27	7	P
12	4	Type IV	28	8	Type IV
13	4	C_{13}	29	7	P
14	4	Type IV	30	8	Type IV
15	4	P	31	7 or 8	?
16	5	FSD	32	8	Type IV

5 Optimal Euclidean Self-Dual Codes

In this section, we consider optimal Euclidean self-dual codes and optimal Euclidean Type IV self-dual codes.

By Lemma 1 and Proposition 3, determining the highest minimum weight of Euclidean self-dual codes of length n is equal to determining the highest minimum weight of binary self-dual codes of length n. Moreover if there is a Euclidean self-dual code with minimum weight d then there is a Euclidean Type IV self-dual code with minimum weight d.

In [4], the exact highest minimum weights of binary self-dual codes of lengths up to 60, and lengths $64, 66$ and 68 was determined. For length 62, recently a self-dual code with minimum weight 12 has been found in [8] and the highest minimum weight is 12. Therefore the exact highest minimum Hamming and Lee weights of Euclidean self-dual codes are determined for lengths up to 68.

Acknowledgments. The authors would like to thank Akihiro Munemasa for helpful discussions. The authors would also like to thank Steven T. Dougherty for helpful comments. This research was carried out while the first author was visiting the Department of Mathematical Sciences, Yamagata University. The first author wishes to thank their hospitality and especially Michio Ozeki for his encouragement.

References

[1] C. Bachoc, Application of coding theory to the construction of modular lattices, *J. Combin. Theory Ser. A* **78** (1997), pp. 92–119.

[2] K. Betsumiya and M. Harada, Binary optimal odd formally self-dual codes, *Designs, Codes and Cryptogr.*, (to appear).

[3] A.E. Brouwer, Bounds on the size of linear codes, in *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman (Eds.), Elsevier, Amsterdam (1998) pp. 295–461.

[4] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1990), pp. 1319–1333.

[5] S.T. Dougherty, M. Harada and P. Solé, Self-dual codes over rings and the Chinese remainder theorem, *Hokkaido Math. J.* **28** (1999), pp. 253–283.

[6] 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), pp. 2345–2360.

[7] S.T. Dougherty, P. Gaborit and P. Solé, Self-dual codes over $\mathbb{F}_2 + v\mathbb{F}_2$, (preprint).

[8] M. Harada, Construction of an extremal self-dual code of length 62, *IEEE Trans. Inform. Theory* **45** (1999), pp. 1232–1233.

[9] G. Kennedy and V. Pless, On designs and formally self-dual codes, *Designs, Codes and Cryptogr.* **4** (1994), pp. 43–55.