

Classification of Type II code over GF(4) of some small lengths

名古屋大学多元数理科学研究科 別宮耕一 (Koichi Betsumiya)
Graduate School of Mathematics, Nagoya University

1 Introduction

Let $GF(2^r)$ be the finite field with 2^r elements. Let C be a code over $GF(2^r)$ of length n , which is a subspace of the vector space $GF(2^r)^n$. Let $B = \{b_1, b_2, \dots, b_r\}$ be a basis of $GF(2^r)$ over $GF(2)$. We denote by $\phi_B(a) = (a_1, a_2, \dots, a_r) \in GF(2)^r$ the representation of $a \in GF(2^r)$ over $GF(2)$ with respect to a basis B , that is, $a = \sum_{i=1}^r a_i b_i$. For $u = (u_1, u_2, \dots, u_n) \in GF(2^r)^n$, we also denote by $\phi_B(u)$ the vector in $GF(2)^{rn}$ obtained by concatenating $\phi_B(u_1), \dots, \phi_B(u_n)$. We call $\phi_B(C)$ the *binary image* of C with respect to B . B is called a *trace-orthogonal basis* (TOB) if $\text{Tr}(b_i b_j) = \delta_{ij}$ for $1 \leq i, j \leq r$ where Tr denotes the trace function of $GF(2^r)$ over $GF(2)$.

In 1980's, Pasquier and Wolfmann studied self-dual codes over $GF(2^r)$ whose binary images with respect to a TOB are binary Type II codes (that is, binary doubly-even self-dual codes) including the extended Hamming code and the extended Golay code (cf. [8, 10]). We say that such codes over $GF(2^r)$ are Type II codes with respect to a TOB [4] (see [6] for Type II codes over $GF(4)$). Recently, it has been proved by the author that the Type II property with respect to a TOB for self-dual codes over $GF(2^r)$ is independent of the choice of a TOB [1]. This allows us to call C a Type II code if C is a Type II code with respect to a TOB, without a reference to an explicit TOB. The *binary length* of a code over $GF(2^r)$ of length n is defined by rn , which is the length of its binary image. The Type II codes with binary length up to 24 have been classified (cf. [2, 4, 6]). We refer to [9] for the classification of binary Type II codes. The next problem would be to classify all Type II codes over $GF(2^r)$ for any r with binary length 32.

Theorem 1.1 (Munemasa [7]) *The total number of Type II $GF(2^r)$ -codes of length n is given by*

$$N_{II,r}(n) = \prod_{i=0}^{n/2-2} (2^{r^i} + 1), \tag{1}$$

if $rn \equiv 0 \pmod{8}$ and $n \equiv 0 \pmod{4}$, and 0 otherwise.

The formula (1) is called the mass formula for Type II codes over $\text{GF}(2^r)$. By Theorem 1.1, the possible cases for which there is a Type II code over $\text{GF}(2^r)$ of length n with binary length 32 are $(n, r) = (32, 1)$, $(16, 2)$, $(8, 4)$ and $(4, 8)$. For the cases $(n, r) = (32, 1)$ and $(n, r) = (8, 4)$, the complete classifications are given in [5] and [4], respectively. Furthermore, for the case $(n, r) = (4, 8)$, it is shown that there exists a unique Type II code up to permutation-equivalence [7].

In this paper, we give a classification for the case $(n, r) = (16, 2)$, that is, Type II codes over $\text{GF}(4)$ of length 16. It is the only remaining case to complete the classification of Type II codes with binary length 32.

2 Classification of Type II Codes over $\text{GF}(4)$ of Length 16

In this section, we give a classification of Type II codes of length 16 over $\text{GF}(4) = \text{GF}(2)[\omega]/(\omega^2 + \omega + 1)$. A *bisorted* matrix is constructed by sorted vectors on a lexicographical order with both directions North to South and West to East. We check all the bisorted 8×8 $\text{GF}(4)$ -matrices A 's such that $(I \ A)$ generates a Type II code, where I is the 8×8 identity matrix. It is sufficient to consider such matrices to complete the classification [3]. Indeed, we obtain 82588 distinct Type II codes by the method above. Let C be a code over $\text{GF}(4)$ of length 16, and let

$$\tilde{C} = \{(\hat{c}_1, \hat{c}_2, \dots, \hat{c}_{16}) \mid \text{wt}(c) = 6, c = (c_1, c_2, \dots, c_{16}) \in C\},$$

where $\text{wt}(c)$ is the Hamming weight of c and $\hat{c}_i = 0$ if $c_i = 0$ and $\hat{c}_i = 1$ otherwise. Then \tilde{C} is a non-linear binary code of length 16. We now consider three invariants of codes under the permutation-equivalence:

1. the Hamming weight enumerator $W(C)$,
2. the order $|\text{Aut}(C)|$ of the permutation automorphism group of C ,
3. the order $|\text{Aut}(\tilde{C})|$ of the permutation automorphism group of \tilde{C} .

Calculating the invariants for every code using MAGMA, we find 48 codes D_1, \dots, D_{48} with distinct sets of invariants. The minimum Hamming weight $d(D_i)$ of D_i , the Hamming weight enumerator $W(D_i)$ of D_i and the values $|\text{Aut}(D_i)|$ are listed in Table 1. The weight enumerators are listed in Table 2 where only the coefficients of the monomials $x^{16-i}y^i$ for $i = 3, 4, 6, 7, \dots, 16$ are given. For all weight enumerators, the coefficients of the monomials x^{16} , $x^{15}y$, $x^{14}y^2$ and $x^{11}y^5$ are 1, 0, 0 and 0, respectively. We verified that

Table 1: Properties of the Type II codes over GF(4) of length 16

| | $d(D_i)$ | $W(D_i)$ | $ \text{Aut}(D_i) $ | | $d(D_i)$ | $W(D_i)$ | $ \text{Aut}(D_i) $ |
|----------|----------|----------|---------------------|----------|----------|----------|---------------------|
| D_1 | 3 | W_1 | 497664 | D_{25} | 4 | W_{24} | 5160960 |
| D_2 | 3 | W_2 | 387072 | D_{26} | 4 | W_{25} | 2304 |
| D_3 | 3 | W_3 | 11664 | D_{27} | 4 | W_{26} | 73728 |
| D_4 | 3 | W_4 | 5184 | D_{28} | 4 | W_{27} | 6144 |
| D_5 | 3 | W_5 | 648 | D_{29} | 4 | W_{28} | 576 |
| D_6 | 3 | W_6 | 7776 | D_{30} | 4 | W_{28} | 6144 |
| D_7 | 3 | W_7 | 324 | D_{31} | 4 | W_{28} | 3072 |
| D_8 | 3 | W_8 | 13608 | D_{32} | 4 | W_{29} | 18432 |
| D_9 | 3 | W_9 | 576 | D_{33} | 4 | W_{29} | 18432 |
| D_{10} | 3 | W_{10} | 90 | D_{34} | 4 | W_{30} | 128 |
| D_{11} | 3 | W_{11} | 216 | D_{35} | 4 | W_{30} | 64 |
| D_{12} | 3 | W_{12} | 432 | D_{36} | 4 | W_{31} | 240 |
| D_{13} | 3 | W_{13} | 3456 | D_{37} | 4 | W_{32} | 24 |
| D_{14} | 3 | W_{14} | 34560 | D_{38} | 4 | W_{32} | 144 |
| D_{15} | 3 | W_{15} | 276480 | D_{39} | 4 | W_{32} | 48 |
| D_{16} | 3 | W_{16} | 13824 | D_{40} | 4 | W_{33} | 48 |
| D_{17} | 3 | W_{17} | 12096 | D_{41} | 4 | W_{33} | 96 |
| D_{18} | 3 | W_{18} | 288 | D_{42} | 6 | W_{34} | 96 |
| D_{19} | 3 | W_{19} | 216 | D_{43} | 6 | W_{34} | 384 |
| D_{20} | 3 | W_{20} | 36 | D_{44} | 6 | W_{35} | 16 |
| D_{21} | 3 | W_{21} | 192 | D_{45} | 6 | W_{35} | 336 |
| D_{22} | 3 | W_{22} | 7920 | D_{46} | 6 | W_{35} | 8 |
| D_{23} | 3 | W_{23} | 18 | D_{47} | 6 | W_{35} | 14 |
| D_{24} | 4 | W_{24} | 3612672 | D_{48} | 6 | W_{35} | 24 |

Table 2: The weight enumerators

| i | 3 | 4 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|----------|----|----|-----|------|------|------|-------|------|-------|-------|-------|------|------|
| W_1 | 48 | 12 | 864 | 432 | 54 | 6912 | 5184 | 1296 | 20844 | 20736 | 7776 | 1296 | 81 |
| W_2 | 24 | 48 | 312 | 1080 | 306 | 4032 | 7056 | 4104 | 24840 | 12096 | 7992 | 3240 | 405 |
| W_3 | 24 | 3 | 522 | 360 | 351 | 5952 | 6156 | 5544 | 18165 | 17856 | 7722 | 2520 | 360 |
| W_4 | 18 | 12 | 384 | 522 | 414 | 5232 | 6624 | 6246 | 19164 | 15696 | 7776 | 3006 | 441 |
| W_5 | 12 | 0 | 360 | 300 | 534 | 5376 | 6816 | 7428 | 17136 | 16128 | 7896 | 3012 | 537 |
| W_6 | 12 | 3 | 378 | 252 | 603 | 5184 | 7164 | 6948 | 17757 | 15552 | 8298 | 2772 | 612 |
| W_7 | 9 | 3 | 282 | 405 | 531 | 5112 | 6876 | 8019 | 17325 | 15336 | 7722 | 3375 | 540 |
| W_8 | 9 | 21 | 150 | 837 | 405 | 4440 | 6804 | 8019 | 19731 | 13320 | 7254 | 4095 | 450 |
| W_9 | 6 | 6 | 252 | 366 | 636 | 4752 | 7368 | 8034 | 17778 | 14256 | 8124 | 3306 | 651 |
| W_{10} | 6 | 0 | 264 | 318 | 606 | 5040 | 7104 | 8418 | 16800 | 15120 | 7896 | 3354 | 609 |
| W_{11} | 6 | 3 | 234 | 414 | 567 | 4944 | 7020 | 8514 | 17157 | 14832 | 7722 | 3546 | 576 |
| W_{12} | 6 | 9 | 222 | 462 | 597 | 4656 | 7284 | 8130 | 18135 | 13968 | 7950 | 3498 | 618 |
| W_{13} | 6 | 18 | 132 | 750 | 480 | 4368 | 7032 | 8418 | 19206 | 13104 | 7428 | 4074 | 519 |
| W_{14} | 6 | 30 | 204 | 558 | 756 | 3600 | 8424 | 6498 | 21690 | 10800 | 9036 | 3114 | 819 |
| W_{15} | 12 | 48 | 120 | 1116 | 450 | 3360 | 7632 | 6084 | 24168 | 10080 | 7992 | 3924 | 549 |
| W_{16} | 12 | 12 | 288 | 540 | 486 | 4896 | 6912 | 7236 | 18828 | 14688 | 7776 | 3348 | 513 |
| W_{17} | 3 | 30 | 156 | 567 | 792 | 3432 | 8568 | 6993 | 21522 | 10296 | 9036 | 3285 | 855 |
| W_{18} | 3 | 12 | 144 | 567 | 594 | 4392 | 7344 | 8721 | 18324 | 13176 | 7776 | 3861 | 621 |
| W_{19} | 3 | 3 | 234 | 279 | 711 | 4680 | 7596 | 8433 | 17253 | 14040 | 8298 | 3285 | 720 |
| W_{20} | 3 | 3 | 186 | 423 | 603 | 4776 | 7164 | 9009 | 16989 | 14328 | 7722 | 3717 | 612 |
| W_{21} | 3 | 6 | 204 | 375 | 672 | 4584 | 7512 | 8529 | 17610 | 13752 | 8124 | 3477 | 687 |
| W_{22} | 12 | 3 | 330 | 396 | 495 | 5280 | 6732 | 7524 | 17493 | 15840 | 7722 | 3204 | 504 |
| W_{23} | 3 | 0 | 216 | 327 | 642 | 4872 | 7248 | 8913 | 16632 | 14616 | 7896 | 3525 | 645 |
| W_{24} | 0 | 84 | 336 | 0 | 1854 | 0 | 14112 | 0 | 32004 | 0 | 15120 | 0 | 2025 |
| W_{25} | 0 | 18 | 228 | 192 | 984 | 3648 | 9048 | 7104 | 19926 | 10944 | 9732 | 2688 | 1023 |
| W_{26} | 0 | 36 | 48 | 768 | 750 | 3072 | 8544 | 7680 | 22068 | 9216 | 8688 | 3840 | 825 |
| W_{27} | 0 | 24 | 168 | 384 | 906 | 3456 | 8880 | 7296 | 20640 | 10368 | 9384 | 3072 | 957 |
| W_{28} | 0 | 12 | 96 | 576 | 630 | 4224 | 7488 | 9216 | 18156 | 12672 | 7776 | 4032 | 657 |
| W_{29} | 0 | 12 | 288 | 0 | 1062 | 3840 | 9216 | 6912 | 19212 | 11520 | 10080 | 2304 | 1089 |
| W_{30} | 0 | 6 | 156 | 384 | 708 | 4416 | 7656 | 9024 | 17442 | 13248 | 8124 | 3648 | 723 |
| W_{31} | 0 | 9 | 126 | 480 | 669 | 4320 | 7572 | 9120 | 17799 | 12960 | 7950 | 3840 | 690 |
| W_{32} | 0 | 3 | 138 | 432 | 639 | 4608 | 7308 | 9504 | 16821 | 13824 | 7722 | 3888 | 648 |
| W_{33} | 0 | 3 | 186 | 288 | 747 | 4512 | 7740 | 8928 | 17085 | 13536 | 8298 | 3456 | 756 |
| W_{34} | 0 | 0 | 216 | 192 | 786 | 4608 | 7824 | 8832 | 16728 | 13824 | 8472 | 3264 | 789 |
| W_{35} | 0 | 0 | 168 | 336 | 678 | 4704 | 7392 | 9408 | 16464 | 14112 | 7896 | 3696 | 681 |

$|\text{Aut}(\tilde{D}_{32})|$ and $|\text{Aut}(\tilde{D}_{33})|$ are 7962624 and 36864, respectively. By Table 1, D_1, \dots, D_{48} are not permutation-equivalent. By Theorem 1.1, we have that

$$\begin{aligned} \sum_{i=1}^{48} \frac{16!}{|\text{Aut}(D_i)|} &= 11925737086250 \\ &= N_{II,2}(16). \end{aligned}$$

Thus, we obtain the following:

Theorem 2.1 *There exist 48 Type II codes over $\text{GF}(4)$ of length 16, up to permutation-equivalence.*

Generator matrices of the codes are given in Section 3. The Frobenius automorphism is the field automorphism on $\text{GF}(4)$ defined by $a \mapsto a^2$. Each of these 48 codes is permutation-equivalent to its Frobenius image. Finally, we calculate the binary images of the codes using MAGMA. In Table 3, the binary codes $\phi(C)$ are given and the minimum Hamming weights $d(\phi(C))$ of $\phi(C)$ are also given. We use the notation in [9] for the binary Type II codes of length 32. There exist 7 Type II codes whose binary images are of minimum Hamming weight 8 up to permutation-equivalence. Only 4 codes among the 5 extremal binary Type II codes of length 32 are the binary images of Type II codes over $\text{GF}(4)$.

As a consequence, we obtain the complete classification of Type II codes over $\text{GF}(2^r)$ with binary length 32. The numbers of Type II codes over $\text{GF}(2^r)$ with binary length 32 up to permutation-equivalence are in Table 4. In the table, #1, #2 and #3 denote the number of codes up to permutation-equivalence, the number of codes whose binary images are extremal, and the number of extremal binary codes obtained as the binary images, respectively.

3 Generator Matrices

In order to save space, we list generator matrices $(I \{a_{i,j}\})$ as

$$a_{1,1}a_{1,2} \cdots a_{1,8}, a_{2,1} \cdots a_{2,8}, \dots, a_{8,1} \cdots a_{8,8},$$

where $\bar{\omega}$ denotes ω^2 .

D_1 : 000000 $\omega\bar{\omega}$, 000000 $\bar{\omega}\omega$, 0000 $\omega\bar{\omega}$ 00, 0000 $\bar{\omega}\omega$ 00, 00 $\omega\bar{\omega}$ 0000, 00 $\bar{\omega}\omega$ 0000, $\omega\bar{\omega}$ 000000, $\bar{\omega}\omega$ 000000

D_2 : 000000 $\omega\bar{\omega}$, 000000 $\bar{\omega}\omega$, 00011100, 00101100, 00110100, 00111000, $\omega\bar{\omega}$ 000000, $\bar{\omega}\omega$ 000000

D_3 : 000000 $\omega\bar{\omega}$, 000000 $\bar{\omega}\omega$, 0000 $\omega\bar{\omega}$ 00, 00 $\omega\bar{\omega}$ 0000, 0 $\omega\bar{\omega}\omega$ 1 $\bar{\omega}$ 00, 0 $\bar{\omega}\omega$ 1 $\bar{\omega}\omega$ 00, ω 01 $\bar{\omega}\bar{\omega}$ 00, $\bar{\omega}$ 0 $\bar{\omega}\omega\omega$ 100

D_4 : 000000 $\omega\bar{\omega}$, 000000 $\bar{\omega}\omega$, 00011100, 00101100, 0 $\omega\bar{\omega}\bar{\omega}\omega$ 100, 0 $\bar{\omega}\omega\omega$ 1 $\bar{\omega}$ 00, ω 0 $\bar{\omega}\bar{\omega}$ 1 ω 00, $\bar{\omega}$ 0 $\omega\omega\bar{\omega}$ 100

D_5 : 000000 $\omega\bar{\omega}$, 0000 $\omega\bar{\omega}$ 00, 000 $\omega\bar{\omega}$ 1 $\bar{\omega}$, 00 ω 01 $\bar{\omega}\bar{\omega}\omega$, 0 $\omega\bar{\omega}$ 100 $\bar{\omega}\omega$, 0 $\bar{\omega}\omega\bar{\omega}$ 00 ω 1, ω 01 $\bar{\omega}\bar{\omega}\omega$ 00, $\bar{\omega}$ 0 $\bar{\omega}\omega\omega$ 100

Table 3: Binary images of the Type II code over GF(4) of length 16

| $\phi(D_i)$ | $d(\phi(D_i))$ | Codes over GF(4) | $\phi(D_i)$ | $d(\phi(D_i))$ | Codes over GF(4) |
|-------------|----------------|-----------------------|-------------|----------------|----------------------------------|
| C5 | 4 | D_{25} | C59 | 4 | D_{11}, D_{29} |
| C10 | 4 | D_{15} | C60 | 4 | D_{10}, D_{36} |
| C17 | 4 | D_{14} | C62 | 4 | D_{21} |
| C24 | 4 | D_1, D_2, D_{24} | C64 | 4 | D_{19}, D_{20} |
| C26 | 4 | D_3, D_4 | C66 | 4 | D_{23} |
| C27 | 4 | D_{16} | C67 | 4 | D_{30}, D_{32}, D_{33} |
| C28 | 4 | D_{22} | C69 | 4 | D_{31} |
| C30 | 4 | D_{27} | C75 | 4 | D_{34}, D_{35} |
| C33 | 4 | D_{13} | C77 | 4 | D_{41} |
| C34 | 4 | D_{28} | C78 | 4 | $D_{37}, D_{38}, D_{39}, D_{40}$ |
| C45 | 4 | D_8, D_{17} | C81 | 8 | D_{46} |
| C51 | 4 | D_6 | C83 | 8 | D_{43}, D_{45} |
| C53 | 4 | D_5, D_{12}, D_{26} | C84 | 8 | D_{47} |
| C55 | 4 | D_7, D_{18} | C85 | 8 | D_{42}, D_{44}, D_{48} |
| C57 | 4 | D_9 | | | |

Table 4: The number of Type II codes with binary length 32

| r | #1 | #2 | #3 | reference |
|-----|----|----|----|-----------|
| 1 | 85 | 5 | 5 | [5] |
| 2 | 48 | 7 | 4 | Section 2 |
| 4 | 6 | 1 | 1 | [4] |
| 8 | 1 | 0 | 0 | [7] |

D_{44} : $000\omega\omega\bar{\omega}1, 00\omega0\bar{\omega}1\bar{\omega}, 0\omega00\bar{\omega}1\omega\bar{\omega}, \omega0001\bar{\omega}\bar{\omega}\omega, \omega\bar{\omega}1\bar{\omega}\omega\omega1, \bar{\omega}\omega\bar{\omega}1\omega\omega1\bar{\omega}, \bar{\omega}1\bar{\omega}\omega1\bar{\omega}\omega\omega, 1\bar{\omega}\omega\bar{\omega}1\omega\omega$
 D_{45} : $000\omega\omega\bar{\omega}1, 00\omega0\bar{\omega}1\bar{\omega}, 0\omega0\omega1\bar{\omega}0\bar{\omega}, \omega0\omega0\bar{\omega}1\bar{\omega}0, \omega\bar{\omega}1\bar{\omega}\omega\omega1, \bar{\omega}\omega\bar{\omega}1\omega\omega1\bar{\omega}, \bar{\omega}10\bar{\omega}1\bar{\omega}1, 1\bar{\omega}\bar{\omega}01\bar{\omega}1\bar{\omega}$
 D_{46} : $000\omega\omega\bar{\omega}1, 00\omega0\bar{\omega}1\bar{\omega}, 0\omega00\bar{\omega}1\omega\bar{\omega}, \omega0\bar{\omega}10\omega0\bar{\omega}, \omega1\bar{\omega}\bar{\omega}\bar{\omega}\omega1, \bar{\omega}\bar{\omega}0\omega1\omega00, \bar{\omega}\bar{\omega}\omega\bar{\omega}0\bar{\omega}0\bar{\omega}, 1\omega1001\bar{\omega}1$
 D_{47} : $000\omega\omega\bar{\omega}1, 00\omega0\bar{\omega}1\bar{\omega}, 0\omega0\omega1\bar{\omega}0\bar{\omega}, \omega0\omega0\bar{\omega}1\bar{\omega}0, \omega1\bar{\omega}\omega\bar{\omega}\omega1, \bar{\omega}\bar{\omega}\omega\omega\omega1\bar{\omega}1, \bar{\omega}\bar{\omega}\omega\omega1\omega1\bar{\omega}, 1\omega\omega\bar{\omega}\omega1\bar{\omega}$
 D_{48} : $000\omega\omega\bar{\omega}1, 00\omega01\bar{\omega}\bar{\omega}, 0\omega0\bar{\omega}\bar{\omega}0\omega1, \omega0\bar{\omega}01\omega0\bar{\omega}, \omega1\bar{\omega}10101, \bar{\omega}\bar{\omega}0\omega10\omega0, \bar{\omega}\bar{\omega}\omega00\omega01, 1\omega1\bar{\omega}1010$

References

- [1] K. Betsumiya, The Type II property for self-dual codes over finite fields of characteristic two, (submitted).
- [2] K. Betsumiya, T. A. Gulliver, M. Harada and A. Munemasa, On Type II codes over \mathbb{F}_4 , *Lecture Notes in Computer Sci.* (to appear).
- [3] K. Betsumiya and M. Harada, Formally self-dual codes related to Type II codes, (submitted).
- [4] K. Betsumiya, M. Harada and A. Munemasa, Type II codes over \mathbb{F}_{2^r} , *IEEE Trans. Inform. Theory* (to appear).
- [5] J.H. Conway, V. Pless and N.J.A. Sloane, The binary self-dual codes of length up to 32, *J. Combin. Theory Ser. A* 60 (1992), 183–195.
- [6] P. Gaborit, V. Pless, P. Solé and O. Atkin, Type II codes over \mathbb{F}_4 , preprint.
- [7] A. Munemasa, Type II codes and quadratic forms over a finite field of characteristic two, *The Ohio State University Mathematical Research Institute Monograph Series*, (to appear).
- [8] G. Pasquier, Binary self-dual codes construction from self-dual codes over a Galois field \mathbb{F}_{2^m} , *Combinatorial mathematics, North-Holland Math. Stud.*, **75**, (1983), 519–526.
- [9] E. M. Rains and N. J. A. Sloane, Self-dual codes, in “Handbook of Coding Theory,” edited by V. Pless and W. C. Huffman, *North Holland, Amsterdam* (1998).
- [10] J. Wolfmann, A class of doubly even self dual binary codes, *Discrete Math.* **56** (1985), 299–303.