Self-Dual Codes over the Integers Modulo 4*

J. H. Conway

Mathematics Department
Princeton University
Princeton, New Jersey 08540

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, New Jersey 07974

ABSTRACT

Michael Klemm has recently studied the conditions satisfied by the complete weight enumerator of a self-dual code over Z_4, the ring of integers modulo 4. In the present paper we deduce analogous theorems for the ''symmetrized'' weight enumerator (which ignores the difference between $+1$ and -1 coordinates) and the Hamming weight enumerator. We give a number of examples of self-dual codes, including codes which realize the basic weight enumerators occurring in all these theorems, and the complete list of self-dual codes of length $n \le 9$. We also classify those self-orthogonal codes that are generated by words of type $\pm 1^4 \; 0^{n-4}$.

1. Introduction

In recent years, several papers have mentioned (implicitly or explicitly) codes over Z_4 ([5]-[8], [20], [21], [26], [31]), without however giving many concrete examples. The main results of the present paper are the following.

The first is a structure theorem (analogous to the result for binary codes stated on p. 35 of [10]) characterizing self-orthogonal[(1)] codes over Z_4 that are generated by ''tetrads'', vectors which contain four components congruent to $+1$ or -1 (mod 4), the other components being congruent to 0 (mod 4). As we shall see later, tetrads are the simplest possible vectors in an indecomposable self-orthogonal code over Z_4.

Theorem 1. Any self-orthogonal code $\#$ over Z_4 generated by tetrads is equivalent to a direct sum of codes from the list

$$\$_{2m} ,\ \$^{O}_{2m} ,\ \$^{+}_{2m} ,\ \$^{\oplus}_{2m} ,\ \ (m = 1, 2, \ldots) ,\ \ \%_7 ,\ \%^{+}_7 ,\ \%_8 \,. \qquad (1)$$

The codes mentioned in (1) are defined in Section 3. They are inequivalent except that $\$^{O}_4 > \$^{+}_4$; the inclusions between these codes are displayed in Figure 1. (The figures are at the end of the paper.)

The second theorem classifies self-dual codes of length up to 9. The statement of this result is facilitated by the fact that self-dual codes over Z_4 have a property not shared by self-dual codes over finite fields: a self-dual code $\#$ of length n can be shortened to a self-dual code of length $n-1$ by deleting any one of its coordinates. This is accomplished as follows. If the projection of $\#$ onto the i-th coordinate contains all of Z_4, the shortened code is obtained by taking those words of $\#$ that are 0 or 2 in the i-th coordinate and omitting that coordinate. If the projection of $\#$ onto the i-th coordinate contains only 0 and 2, we take the words of $\#$ that are 0 in the i-th coordinate and omit that coordinate.

---

* This paper appeared in *J. Combinatorial Theory*, Series A, Vol. 62 (1993), pp. 30-45.

(1) The terms ''self-orthogonal'', ''self-dual'', ''equivalent'', etc. are explained in Section 2.

Theorem 2. Any indecomposable self-dual code over $\mathbb{Z}_4$ of length $n \le 9$ is equivalent to one of those shown in Table I. All self-dual codes of length $n \le 8$ are shown in Figure 2, in which a line indicates that the upper code can be obtained by shortening the lower code.

Table I. All indecomposable self-dual codes over $\mathbb{Z}_4$ of length $n \le 9$.

$\#$	n	$\lvert\#\rvert$	$\lvert G\rvert$	swe
$!_1$	1	2^1	2	$1+c$
$\$_4^{\oplus}$	4	$4^1 2^2$	$2^3 \cdot 4!$	$1+6c^2+8b^4+c^4$
$\$_6^{\oplus}$	6	$4^2 2^2$	$2^6 \cdot 6$	$1+3c^2+8c^3+12b^4+3c^4+\cdots$
$\%_7^{+}$	7	$4^3 2^1$	$2 \cdot 168$	$1+7c^3+14b^4+7c^4+\cdots$
$\$_8^{\oplus}$	8	$4^3 2^2$	$2^8 \cdot 8$	$1+4c^2+16b^4+22c^4+\cdots$
$\%_8$	8	4^4	$8 \cdot 2 \cdot 4!$	$1+16b^4+14c^4+48b^4c+\cdots$
$-_8$	8	$4^1 2^6$	$2^7 \cdot 8!$	$1+28c^2+70c^4+28c^6+\cdots$
$-_8'$	8	$4^2 2^4$	$2^7 (4!)^2$	$1+12c^2+38c^4+64b^4c+\cdots$
2_8	8	4^4	1344	$1+14c^4+112b^4c+112b^4c^3+\cdots$
4_8	8	$4^3 2^2$	$2^8 \cdot 4!$	$1+4c^2+22c^4+96b^4c+\cdots$

For the proofs of Theorems 1 and 2 see Section 3.

In [21], Klemm has studied the conditions satisfied by the complete weight enumerators of self-dual codes over $\mathbb{Z}_4$ (see Theorems 4, 5 below). In Section 2 we deduce analogous theorems for the ‘‘symmetrized’’ and Hamming weight enumerators (see Theorems 6-9), and in Table II we list examples of self-dual codes that realize the basic weight enumerators occurring in all these theorems. The codes themselves are defined in Section 3. Theorem 3 is a general result on obtaining codes over $\mathbb{Z}_4$ from pairs of binary codes.

2. Codes over $\mathbb{Z}_4$

We first establish some terminology. By a ‘‘code’’ $\#$ we usually mean an additive subgroup of $\mathbb{Z}_4^n$. We define an inner product on $\mathbb{Z}_4^n$ by $x \cdot y = x_1 y_1 + \cdots + x_n y_n$ (mod 4), and the notions of *dual* code ($\#^*$), *self-orthogonal* code ($\# \subseteq \#^*$) and *self-dual* code ($\# = \#^*$) are then defined in the standard way (cf. [20], [24]). For most applications there is no need to distinguish between $+1$ components of codewords and -1 components, and so we say that two codes are *equivalent* (denoted $>$) if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. Codes differing by only a permutation of coordinates are called *permutation-equivalent.* The automorphism group $\mathrm{Aut}(\#)$ of $\#$ consists of all permutations and sign-changes of the coordinates that preserve the set of codewords. We denote the order of $\mathrm{Aut}(\#)$ by g.

Any code is permutation-equivalent to a code $\#$ with generator matrix of the form

$$\begin{bmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{bmatrix} \tag{2}$$

where A, B are matrices over $\mathbb{Z}_4$ and C is a $\{0,1\}$-matrix. The code is then an elementary abelian group of type $4^{k_1} 2^{k_2}$, containing $2^{2k_1+k_2}$ codewords. We shall indicate this by writing $\lvert\#\rvert = 4^{k_1} 2^{k_2}$.

The dual code $\#^*$ to (2) has generator matrix

$$\begin{bmatrix} -B^{tr} - C^{tr}A^{tr} & C^{tr} & I_{n-k_1-k_2} \\ 2A^{tr} & 2I_{k_2} & 0 \end{bmatrix} \qquad (3)$$

and $|\#^*| = 4^{n-k_1-k_2} 2^{k_2}$.

Suppose L (resp. L^*) is the lattice consisting of all integer points congruent modulo 4 to the words of C (resp. C^*). Then the invariant factors of L are

$$4^{k_1} 2^{k_2} 1^{n-k_1-k_2}$$

and for L^* they are

$$4^{n-k_1-k_2} 2^{k_2} 1^{k_1} \ .$$

Let β be the ''mod 2'' map from Z_4 to Z_2, sending 0 and 2 to 0, 1 and 3 to 1. The kernel $\{0,2\}$ is isomorphic to Z_2, and we denote this isomorphism by γ, so that $\gamma(0)=0$, $\gamma(2)=1$.

There are two binary codes $\#^{(1)}$, $\#^{(2)}$ canonically associated with $\#$:

$$\#^{(1)} = \{ \beta(u) \, : \, u \in \# \} \ ,$$
$$\#^{(2)} = \{ \gamma(u) \, : \, u \in \# \, , \, \beta(u) = 0 \} \ .$$

$\#^{(1)}$ is an $[n, \, k_1]$ binary code which (if $\#$ is defined by (2)) has generator matrix

$$[I_{k_1} \quad \beta(A) \quad \beta(B)] \ , \qquad (4)$$

while $\#^{(2)} \supseteq \#^{(1)}$ is an $[n, \, k_1 + k_2]$ binary code with generator matrix

$$\begin{bmatrix} I_{k_1} & \beta(A) & \beta(B) \\ 0 & I_{k_2} & C \end{bmatrix} . \qquad (5)$$

If $\#$ is self-orthogonal then $\#^{(1)}$ is a self-orthogonal doubly-even binary code and $\#^{(1)} \subseteq \#^{(2)} \subseteq \#^{(1)*}$. Furthermore if $\#$ is self-dual then $\#^{(2)} = \#^{(1)*}$. The next theorem gives the converse assertions.

Theorem 3. If $!$, $@$ are binary codes with $! \subseteq @$ then there is a code $\#$ over Z_4 with $\#^{(1)} = !$, $\#^{(2)} = @$. If in addition $!$ is self-orthogonal and doubly-even and $@ \subseteq !^*$ then there is a self-orthogonal code $\#$ over Z_4 with $\#^{(1)} = !$, $\#^{(2)} = @$. Furthermore if $@ = !^*$ then $\#$ is self-dual.

Proof. Let $\dim ! = k_1$, $\dim B = k_1 + k_2$. Without loss of generality we may assume that $!$, $@$ have generator matrices

$$[I \quad X \quad Y] \ , \qquad \begin{bmatrix} I & X & Y \\ 0 & I & Z \end{bmatrix}$$

respectively. Then

$$\begin{bmatrix} I & X & Y \\ 0 & 2I & 2Z \end{bmatrix} \qquad (6)$$

is a generator matrix for a code $\#$ with $\#^{(1)} = !$, $\#^{(2)} = @$. To establish the second assertion we must modify (6) to make $\#$ self-orthogonal. This is accomplished by replacing the (j,i)-th entry of (6) by the inner product modulo 4 of rows i and j, for $1 \le i \le k_1$, $1 \le j \le k_1 + k_2$, $i < j$. ∎

In this way every self-*orthogonal* doubly-even binary code corresponds to one or more self-*dual* codes over Z_4. For example the vectors

$$3(20000101001100110101111) \tag{7}$$

– where the parentheses indicate that all cyclic shifts of the parenthesized portion(s) are to be used – generate a self-dual code $\&_{24}$ over Z_4 for which $\&_{24}^{(1)} = \&_{24}^{(2)}$ is the binary Golay code.

The *complete weight enumerator* (or c.w.e.) of $\#$ is

$$\mathrm{cwe}_{\#}(a,b,c,d) = \sum_{u \in \#} a^{n_0(u)} b^{n_1(u)} c^{n_2(u)} d^{n_3(u)} , \tag{8}$$

where $n_i(u)$ is the number of components of u that are congruent to i (mod 4) (cf. [20], [24, p. 141]). Permutation-equivalent codes have the same c.w.e., but equivalent codes may have distinct c.w.e.'s. The appropriate weight enumerator for an equivalence class of codes is what we shall call the *symmetrized weight enumerator* (or s.w.e.), obtained by identifying b and d in (8):

$$\mathrm{swe}_{\#}(a,b,c) = \mathrm{cwe}_{\#}(a,b,c,b) . \tag{9}$$

This is equivalent to the ''weight function'' $W(Z_1, Z_2, Z_4)$ of Klemm [20]. The *Hamming weight enumerator* of $\#$ is

$$W_{\#}(a,b) = \mathrm{cwe}_{\#}(a,b,b,b) . \tag{10}$$

The theorems stated below require that we work with homogeneous polynomials, but sometimes – as in Table I – it is simpler to set $a = 1$.

There are several other criteria for judging a code $\#$ over Z_4 besides its minimal Hamming weight. One may consider its minimal *Euclidean norm*, defined by $N(0) = 0$, $N(\pm 1) = 1$, $N(2) = 4$ (cf. [4]), which can be found from $\mathrm{swe}_{\#}(1,x,x^4)$. In [13] (see also [9], [14]) the Leech lattice was constructed by combining eight copies of the face-centered cubic lattice using the code $\# = 2_8$. For this type of construction one needs the minimal A_3-*norm* of $\#$, defined by $N(0) = 0$, $N(\pm 1) = 3/4$, $N(2) = 1$, which can be found from $\mathrm{swe}_{\#}(1,x^{3/4},x)$.

Klemm [21, Theorem 1.5] gives an analog of the MacWilliams identity:

$$\mathrm{cwe}_{\#^*}(a,b,c,d) = \frac{1}{|\#|} \mathrm{cwe}_{\#}(a+b+c+d,\ a+ib-c-id,\ a-b+c-d,\ a-ib-c+id) , \tag{11}$$

which implies

$$\mathrm{swe}_{\#^*}(a,b,c) = \frac{1}{|\#|} \mathrm{swe}_{\#}(a+2b+c,\ a-c,\ a-2b+c) \tag{12}$$

(this is also a special case of Theorem 1.2 of Klemm [20]), and

$$W_{\#^*}(a,b) = \frac{1}{|\#|} W_{\#}(a+3b,\ a-b) . \tag{13}$$

Klemm observes that (11) is simpler when stated in terms of the variables

$$\overline{a} = \frac{a+c}{\sqrt{2}},\ \ \overline{b} = \frac{b+d}{\sqrt{2}},\ \ \overline{c} = \frac{a-c}{\sqrt{2}},\ \ \overline{d} = \frac{b-d}{\sqrt{2}} . \tag{14}$$

Let $\overline{\mathrm{cwe}}_{\#}$ denote the c.w.e. of $\#$ when written as a function of $\overline{a}$, $\overline{b}$, $\overline{c}$, $\overline{d}$. Then (11) implies ([21, Theorem 1.5])

$$\overline{\mathrm{cwe}}_{\#^*}(\overline{a},\overline{b},\overline{c},\overline{d}) = \frac{2^n}{|\#|} \overline{\mathrm{cwe}}_{\#}(\overline{a},\overline{c},\overline{b},i\overline{d}) . \tag{15}$$

The main results of [21] are the following two theorems.

Theorem 4 (Klemm [21]). The c.w.e. of a self-dual code over $\mathbb{Z}_4$ belongs to the ring

$$\mathbb{C}[\theta_1, \theta_{4a}, \theta_{4b}, \theta_8] \oplus \theta_{10}\, \mathbb{C}[\theta_1, \theta_{4a}, \theta_{4b}, \theta_8] \,, \tag{16}$$

where

$$\theta_1 = \bar{a},\ \theta_{4a} = (\bar{b}^4 + \bar{c}^4),\ \theta_{4b} = \bar{d}^4 \,,$$
$$\theta_8 = \bar{b}^4 \bar{c}^4,\ \theta_{10} = (\bar{b}\bar{c}\bar{d})^2 (\bar{b}^4 - \bar{c}^4) \,. \tag{17}$$

This ring has the Molien series (cf. [24], [27])

$$\frac{1+\lambda^{10}}{(1-\lambda)(1-\lambda^4)^2(1-\lambda^8)} \,. \tag{18}$$

Theorem 5 (Klemm [21]). The c.w.e. of a self-dual code over $\mathbb{Z}_4$ that contains the all-ones vector belongs to the ring

$$R \oplus \sigma_8 R \oplus \sigma_8^2 R \oplus \sigma_{16} R \oplus \sigma_8 \sigma_{16} R \oplus \sigma_8^2 \sigma_{16} R \tag{19}$$

where R is the ring of symmetric functions of $\bar{a}^4$, $\bar{b}^4$, $\bar{c}^4$, $\bar{d}^4$, and

$$\sigma_8 = \bar{a}^4 \bar{d}^4 + \bar{b}^4 \bar{c}^4 \,,$$
$$\sigma_{16} = (\bar{a}\bar{b}\bar{c}\bar{d})^2 (\bar{a}^4 \bar{b}^4 + \bar{c}^4 \bar{d}^4 - \bar{a}^4 \bar{c}^4 - \bar{b}^4 \bar{d}^4) \,. \tag{20}$$

This ring has the Molien series

$$\frac{(1+\lambda^8+\lambda^{16})(1+\lambda^{16})}{(1-\lambda^4)(1-\lambda^8)(1-\lambda^{12})(1-\lambda^{16})} \,. \tag{21}$$

The analogous theorems for symmetric and Hamming weight enumerators follow easily from Theorems 4 and 5; we omit the proofs.

Theorem 6. The s.w.e. of a self-dual code over $\mathbb{Z}_4$ belongs to the ring

$$\mathbb{C}[\tilde{a},\ \tilde{b}^4 + \tilde{c}^4,\ \tilde{b}^4 \tilde{c}^4] \,, \tag{22}$$

where

$$\tilde{a} = \frac{a+c}{\sqrt{2}},\quad \tilde{b} = \sqrt{2}\, b,\quad \tilde{c} = \frac{a-c}{\sqrt{2}} \,. \tag{23}$$

This ring has the Molien series

$$\frac{1}{(1-\lambda)(1-\lambda^4)(1-\lambda^8)} \,. \tag{24}$$

An alternative basis is given by the polynomials

$$\phi_1 = a + c \,,$$
$$\phi_4 = 2b^4 - ac(a^2 + c^2) \,, \tag{25}$$
$$\phi_8 = b^4 (a-c)^4 \,.$$

Theorem 7. The s.w.e. of a self-dual code of length n over $\mathbb{Z}_4$ containing a vector $\pm 1^n$ belongs to the ring

$$S \oplus \tilde{b}^4 \tilde{c}^4 S \oplus \tilde{b}^8 \tilde{c}^8 S \,, \tag{26}$$

where S is the ring of symmetric functions of $\tilde{a}^4$, $\tilde{b}^4$, $\tilde{c}^4$. This ring has the Molien series

$$\frac{1+\lambda^8+\lambda^{16}}{(1-\lambda^4)(1-\lambda^8)(1-\lambda^{12})} \,. \tag{27}$$

An explicit basis for S is given by the polynomials

$$\begin{aligned} \Phi_4 &= a^4+6a^2c^2+8b^4+c^4 \,, \\ \Phi_8 &= (a^2c^2-b^4)((a^2+c^2)^2-4b^4) \,, \\ \Phi_{12} &= b^4(a^2-c^2)^4 \,, \end{aligned} \tag{28}$$

and then the ring is $S \oplus \Psi_8 S \oplus \Psi_8^2 S$, where

$$\Psi_8 = b^4(a-c)^4 \,, \tag{29}$$

with

$$\Psi_8^3 = \Psi_8^2 \left(\frac{1}{16} \Phi_4^2 - \Phi_8 \right) - \frac{1}{8} \Psi_8 \Phi_4 \Phi_{12} + \frac{1}{16} \Phi_{12}^2 \,. \tag{30}$$

Theorem 8. The Hamming weight enumerator of a self-dual code over $\mathbb{Z}_4$ belongs to the ring

$$\mathbb{C}[w_1, w_4] \oplus w_8 \, \mathbb{C}[w_1, w_4] \,, \tag{31}$$

where

$$\begin{aligned} w_1 &= a+b \,, \\ w_4 &= ab(a^2+b^2)-2b^4 \,, \\ w_8 &= b^4(a-b)^4 \,, \end{aligned} \tag{32}$$

and

$$w_8^2 = w_8(w_1^8-4w_1^4w_4+2w_4^2) - w_4^4 \,. \tag{33}$$

This ring has the Molien series

$$\frac{1+\lambda^8}{(1-\lambda)(1-\lambda^4)} \,. \tag{34}$$

Theorem 9. The Hamming weight enumerator of a self-dual code of length n over $\mathbb{Z}_4$ containing a vector $\pm 1^n$ belongs to the ring

$$\mathbb{C}[W_4, W_8] \oplus X_8 \mathbb{C}[W_4, W_8] \oplus X_{12} \mathbb{C}[W_4, W_8] \oplus X_8 X_{12} \mathbb{C}[W_4, W_8] \,, \tag{35}$$

where

$$
\begin{aligned}
W_4 &= (a^2+3b^2)^2 \ , \\
W_8 &= b^4(a-b)^4 \ , \\
X_8 &= b^2(a^2-b^2)^2(a^2+3b^2) \ , \\
X_{12} &= b^4(a^2-b^2)^4 \ ,
\end{aligned}
\tag{36}
$$

with

$$
X_8^2 = W_4 X_{12} \ ,
$$

$$
X_{12}^2 = 2X_{12}W_4W_8 + W_8^2(16X_8 - W_4^2) + 16W_8^3 \ . \tag{37}
$$

This ring has the Molien series

$$
\frac{(1+\lambda^8)(1+\lambda^{12})}{(1-\lambda^4)(1-\lambda^8)} \ . \tag{38}
$$

A question left unanswered by Klemm in [21] is whether one can find a set of codes with lengths equal to the degrees of the basic polynomials in Theorems 4 and 5 and whose c.w.e.'s are a polynomial basis for the rings (16) and (19). In other words, are there analogues of Gleason's theorem that says (for example) that the weight enumerator of a self-dual doubly-even binary code is a polynomial in the weight enumerators of the Hamming and Golay codes (cf. [3], [16], [23], [24], [27])? Similar questions can be asked about Theorems 6-9.

The affirmative answers to these questions are obtained using the codes listed in Table II.

Table II

Theorem	Corresponding codes
4	$!_1$, $\$_4^{\oplus}$ in two versions (39a), (39b), 2_8 (41); $\#_{10}$ (45).
5	$—_4$, $—_8$, $—_{12}$, $—_{16}$ (43); 2_8 (41), $\#_{16}$ (46).
6	$!_1$, $\$_4^{\oplus}$, 2_8.
7	$—_4$, $—_8$, $—_{12}$; 2_8.
8	$!_1$, $\$_4^{\oplus}$; 2_8.
9	$—_4$, 2_8; $—_8$, $—_{12}$.

The codes mentioned in Table II are defined in Section 3. In general we use the same name for all codes in an equivalence class, but for the first two lines of Table II we include equation numbers to identify particular representatives from the equivalence classes. The codes before the semicolons have algebraically independent weight enumerators, and correspond to the terms in the denominators of the Molien series (18), (21), etc., while those after the semicolon correspond to the terms in the numerator. We discuss this table further in Section 3.

3. Examples of self-orthogonal and self-dual codes over Z_4

The smallest self-dual code is $!_1 = \{0,2\}$, with symmetrized weight enumerator $a+c$ and $g = |\mathrm{Aut}(!_1)| = 2$ (the transformation that negates all coordinates is always in $\mathrm{Aut}(\#)$).

If a self-orthogonal code $\#$ contains a vector of type $2^1 0^{n-1}$ then $\# > !_1 \oplus \#'$ is decomposable. The next-simplest possible vectors are ''tetrads'', of type $\pm 1^4 0^{n-4}$ (see Section 1). We now list a number of self-orthogonal codes that are generated by tetrads; t denotes the total number of tetrads in the code.

The first four codes have the property that the associated binary code $\#^{(1)}$ is the self-dual code d_{2m} of [10], [12].

$\$_{2m}$ ($m \geq 2$ – the subscript gives the length) is generated by the tetrads 11130...0, 0011130...0, ..., 0...01113; $|\$_{2m}| = 4^{m-1}$, $g = 2 \cdot 4!$ $(m=2)$ or $2^2 \cdot 2^m$ $(m > 2)$, $t = 2(m-1)$. $\$_{2m}^{*}/\$_{2m}$ is a group of type 4^2 with generators $v_1 = 0101...01$, $v_2 = 00...0011$.

$\$_{2m}^{\mathrm{O}}$ ($m \geq 2$) is generated by $\$_{2m}$ and the tetrad 1300...0011 (or equivalently the vector 2020...20); $|\$_{2m}^{\mathrm{O}}| = 4^{m-1}2$, $g = 2^2 \cdot 8(m=2)$ or $2 \cdot 2^{m-1} \cdot 2m$ $(m > 2)$, $t = 2m$. $(\$_{2m}^{\mathrm{O}})^{*}/\$_{2m}^{\mathrm{O}}$ is a cyclic group of order 4 generated by v_1 (if m is odd), or a 4-group generated by v_1 and $2v_2$ (if m is even).

$\$_{2m}^{+}$ ($m \geq 2$, but note that $\$_4^{+} > \$_4^{\mathrm{O}}$) is generated by $\$_{2m}$ and $2v_2$; $|\$_{2m}^{+}| = 4^{m-1}2$, $g = 2^m \cdot 2^{m+1}$, $t = 4(m-1)$. $(\$_{2m}^{+})^{*}/\$_{2m}^{+}$ is a 4-group generated by $2v_1$ and v_2.

$\$_{2m}^{\oplus}$ ($m \geq 2$) is the self-dual code generated by $\$_{2m}^{\mathrm{O}}$ and $\$_{2m}^{+}$; $|\$_{2m}^{\oplus}| = 4^{m-1}2^2$, $g = 2^3 \cdot 4!$ $(m=2)$ or $2^m \cdot 2^m \cdot 2m$ $(m > 2)$, $t = 4m$. For use in Table II we note that there are two permutation-inequivalent versions of $\$_4^{\oplus}$, with generator matrices

$$(a) \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{bmatrix}, \qquad (b) \quad \begin{bmatrix} 1 & 3 & 3 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{bmatrix}. \tag{39}$$

$\$_4^{\oplus}$ (in either version) has swe $= a^4 + 6a^2c^2 + c^4 + 8b^4$.

$\%_7$ is generated by 1003110, 1010031, 1101003; $|\%_7| = 4^3$, $g = 2 \cdot 4!$, $t = 8$. $\%_7^{*}/\%_7$ is a cyclic group of order 4 generated by 3111111.

$\%_7^{+}$ is the self-dual code generated by $\%_7$ and 2222222 (or equivalently by all cyclic shifts of 3110100); $|\%_7^{+}| = 4^3 2$, $g = 2 \cdot 168$, $t = 14$, swe $= a^7 + c^7 + 14b^4(a^3 + c^3) + 7a^3c^3(a+c) + 42ab^4c(a+c)$. For both $\%_7$ and $\%_7^{+}$ the associated binary code $\#^{(1)}$ is the dual Hamming code e_7.

$\%_8$ is the self-dual code generated by $0u$, $u \in \%_7$ and 30001011, or equivalently is the code defined by the generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 3 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 3 & 3 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 3 & 0 \end{bmatrix}; \tag{40}$$

$|\%_8| = 4^4$, $g = 8 \cdot 2 \cdot 4! = 384$, $t = 16$, swe $= a^8 + 16b^8 + c^8 + 16b^4(a^4 + c^4) + 14a^4c^4 + 48ab^4c(a^2 + c^2) + 96a^2b^4c^2$.

Proof of Theorem 1. It is now easy to verify (using Figure 1 as a guide) that the preceding codes are, up to equivalence, the only ones generated by tetrads; we omit the details.

We next list some further examples of self-dual codes.

The *octacode* 2_8 (cf. [9], [13], [14]) is the self-dual code generated by the vectors

$$3(2001011), \tag{41}$$

or equivalently is the code defined by the generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 3 & 2 & 1 & 3 \\ 0 & 0 & 1 & 0 & 3 & 3 & 2 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 3 & 2 \end{bmatrix}; \tag{42}$$

$|2_8| = 4^4$, $g = 1344$, $t=0$, swe $= a^8 + 16b^8 + c^8 + 14a^4c^4 + 112ab^4c(a^2+c^2)$. For both $\%_8$ and 2_8 the associated binary code $\#^{(1)}$ is the Hamming code e_8.

The matrices (40) and (42) may be generalized as follows. Let H_n be a skew-type Hadamard matrix of order $n \equiv 0 \pmod 4$ ([19, p. 244], [30, pp. 292, 451, 459]), with $H_n = I_n + S_n$, $S_n = -S_n^{tr}$, $S_n S_n^{tr} = (n-1) I_n$. Then both $[I_n | S_n]$ and $[I_n | S_n + 2I_n]$ are generator matrices for self-dual codes of length $2n$. Examples are known for $n = 4, 8, 12, \ldots, 112$.

4_8 is the self-dual code obtained by taking the 16-word code generated by all even permutations of 0123 and replacing 0 by 00 or 22, 1 by 11 or 33, 2 by 02 or 20 and 3 by 13 or 31. 4_8 has generator matrix

$$\begin{bmatrix} 00 & 11 & 02 & 13 \\ 00 & 02 & 13 & 11 \\ 11 & 02 & 00 & 13 \\ 02 & 02 & 02 & 02 \\ 00 & 00 & 00 & 22 \end{bmatrix};$$

$|4_8| = 4^3 2^2$, $g = 2^8 \cdot 4! = 6144$, $t=0$, swe $= a^8 + 32b^8 + c^8 + 4a^2c^2(a^4+c^4) + 22a^4c^4 + 96ab^4c(a^2+c^2)$.

$\__{4m}$ ($m \geq 1$, but note that $\__4 > \$_4^{\oplus}$) is a self-dual code introduced by Klemm [21], having generator matrix

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 2 & 0 & \cdots & 0 & 2 \\ 0 & 0 & 2 & \cdots & 0 & 2 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 2 & 2 \end{bmatrix}; \tag{43}$$

$|\__{4m}| = 4^1 2^{4m-2}$, $g = 2^{4m-1}(4m)!$, cwe $= 2^{2m-1}(\bar{a}^{4m} + \bar{b}^{4m} + \bar{c}^{4m} + \bar{d}^{4m})$ (see (14)).

More generally, given any graph G with k vertices labeled by positive integers $m_1, \ldots, m_k$ and node-node adjacency matrix $A = (a_{ij})$, there is a self-dual code of length $n = 4m_1 + \cdots + 4m_k$ generated by (i) the vectors

$$v_i = v_{i1} \cdots v_{ik}, \qquad (1 \leq i \leq k),$$

where $v_{ii} = 1^{4m_i}$, $v_{ij} = 0^{4m_j}$ if $a_{ij} = 0$ or $v_{ij} = 0^{4m_j - 1}2$ if $a_{ij} = 1$, together with (ii) the vectors that have evenly many 2's on each of the k coordinate blocks. $\__{4m}$ itself is the case where G consists of a single vertex. When G consists of a single edge joining a pair of vertices labeled 1 we obtain a code $\_'_8$ with generator matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 2 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{bmatrix}; \tag{44}$$

$|\_'_8| = 4^2 2^4$, $g = 2 \cdot 2^6 \cdot (4!)^2 = 73728$, $t=0$, swe $= a^8 + 64b^8 + c^8 + 12a^2c^2(a^4+c^4) + 38a^4c^4 + 64ab^4c(a^2+c^2)$.

$\#_{10}$ is the self-dual code with generator matrix

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 3 & 3 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 \end{bmatrix}, \tag{45}$$

and $|\#_{10}| = 4^2 2^6$. This code, used in Table II, was found as a ''neighbor'' (defined as in [15]) of the direct sum of $d_4^{\oplus}$ and $d_6^{\oplus}$.

Let A be the point-block incidence matrix of a symmetric (v,k,λ)-design for which λ is odd and $k-\lambda \equiv 4 \pmod 8$. Klemm [20], [21] shows that the rows of A span a code $\#$ of length v with $\# = \langle \#^*, 1^v \rangle$, and that $\langle \#^*, 2^v \rangle$ is self-dual. If in addition $\lambda \equiv 3 \pmod 4$ then, by adding an extra coordinate to $\#$ to make the sum of the coordinates zero, we obtain a self-dual code $\$_{v+1}$ containing 1^{v+1}.

For example, any normalized Hadamard matrix H_n of order $n \equiv 16 \pmod{32}$ produces a self-dual code $\$_n$ of length n. $\$_n$ is generated by the vector 1^n and the rows of the matrix obtained from H_n by replacing $+1$ entries by 0 and -1 entries by 1.

There are five distinct Hadamard matrices of order 16 ([1], [2], [4], [17], [18], [25], [29]), from which we obtain five self-dual codes $\$_{16}$ of length 16. These are inequivalent, since the associated binary codes $\$_{16}^{(1)}$ have been shown by Assmus and Key [2] to be inequivalent. Unfortunately none of the c.w.e.'s of these five codes involves the polynomial σ_{16} of Theorem 5. However, by taking a neighbor of the second code $\$_{16}$ (in the Assmus-Key ordering [2]), we obtain a self-dual code $\#_{16}$ with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 3 & 3 & 1 & 0 & 3 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 3 & 3 & 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 3 & 3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 3 & 0 & 2 & 3 & 3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 3 & 2 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 \end{bmatrix}, \tag{46}$$

whose c.w.e. does involve σ_{16}.

Notes on Table II. We illustrate Table II by expressing the symmetrized weight enumerators of the codes in the fourth line of the table in terms of the basic polynomials given in Theorem 7:

$$\begin{aligned} \mathrm{swe}_{-4} &= \Phi_4 , \\ \mathrm{swe}_{-8} &= \Phi_8 + 16\Phi_4^2 , \\ \mathrm{swe}_{-12} &= 24\Phi_{12} + 48\Phi_4\Phi_8 + \Phi_4^3 , \\ \mathrm{swe}_{2_8} &= -28\Psi_8 - 12\Phi_8 + \Phi_4^2 . \end{aligned}$$

Proof of Theorem 2. Let $\#$ be an indecomposable self-dual code of length $n \geq 2$, and let $\#^{(1)}$ be the associated binary code. The projection of $\#$ onto any coordinate must be all of Z_4 (for otherwise $\#^* = \#$ contains a subcode isomorphic to $!_1$ and is decomposable). $\#^{(1)}$ is therefore a binary self-orthogonal doubly-even code in which no coordinate position is identically zero. There are no such codes of lengths 2, 3, 5 or 9.

For length 4 we have $\#^{(1)} = d_4 = \{0^4, 1^4\}$, which forces $\# > \$_4^{\oplus} > \_\,_4$. In general, if dim $\#^{(1)} = 1$, then $\# > \_\,_n$.

For lengths 6, 7, 8 and dim $\#^{(1)} \geq 2$, $\#^{(1)}$ is one of d_6, e_7, d_4^2, d_8 or e_8, and it is not difficult to show that the codes listed in Table I are the only possibilities for $\#$. ■

We end with a question: is there a ''mass formula'' for self-dual codes over Z_4, analogous to those for codes over $GF(2)$ ([24[2], Chap. 19, Cors. 19 and 23], [28, (9.1.1) and (9.1.2)]), $GF(3)$ ([11, p. 313], [28, (9.1.3)]), $GF(4)$ ([11, p. 313], [28, (9.1.4)]), and $GF(5)$ ([22])?

Acknowledgements

We thank E. F. Assmus, Jr., T. Etzion and M. Klemm for helpful comments.

(2) In equations (74), (75), (76) on p. 631 of [24] the initial 2 should be deleted.

REFERENCES

[1] E. F. Assmus, Jr., ‘‘On the theory of design’’, in *Surveys in Combinatorics, 1989*, ed. J. Siemons, Camb. Univ. Press, 1989. London Mathematical Society Lecture Note Series 141, pp. 1-21.

[2] E. F. Assmus, Jr. and J. D. Key, ‘‘Hadamard matrices and their designs: a coding theoretic approach’’, Trans. Amer. Math. Soc., to appear.

[3] E. R. Berlekamp, F. J. MacWilliams and N. J. A. Sloane, ‘‘Gleason’s theorem on self-dual codes’’, IEEE Trans. Information Theory, **18** (1972), 409-414.

[4] V. N. Bhat and S. S. Shrikhande, ‘‘Non-isomorphic solutions of some balanced incomplete block designs I’’, J. Combinatorial Theory, **9** (1970), 174-191.

[5] I. F. Blake, ‘‘Codes over certain rings’’, Info. Control, **20** (1972), 396-404.

[6] I. F. Blake, ‘‘Codes over integer residue rings’’, Info. Control, **29** (1975), 295-300.

[7] E. H. Brown, Jr., ‘‘Generalizations of the Kervaire invariant’’, Ann. Math., **95** (1972), 368-383.

[8] A. R. Calderbank and G. J. Pottie, ‘‘Upper bounds for small trellis codes’’, preprint.

[9] J. H. Conway, R. A. Parker and N. J. A. Sloane, ‘‘The covering radius of the Leech lattice’’, Proc. Royal Soc. London, Series A, **380** (1982), 261-290. A revised version appears as Chapter 23 of [14].

[10] J. H. Conway and V. Pless, ‘‘On the enumeration of self-dual codes’’, J. Combinatorial Theory, Series A, **28** (1980), 26-53. See [12] for errata.

[11] J. H. Conway, V. Pless and N. J. A. Sloane, ‘‘Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16’’, IEEE Trans. Information Theory, **25** (1979), 312-322.

[12] J. H. Conway, V. Pless and N. J. A. Sloane, ‘‘The binary self-dual codes of length up to 32: a revised enumeration’’, J. Combinatorial Theory, Series A, to appear.

[13] J. H. Conway and N. J. A. Sloane, ‘‘Twenty-three constructions for the Leech lattice’’, Proc. Royal Soc. London, Series A, **381** (1982), 275-283. A revised version appears as Chapter 24 of [14].

[14] J. H. Conway and N. J. A. Sloane, ‘‘Sphere Packings, Lattices and Groups’’, Springer-Verlag, NY, 1988.

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

[16] A. M. Gleason, ‘‘Weight polynomials of self-dual codes and the MacWilliams identities’’, Actes, Congrès Intern. Math., Gauthiers-Villars, Paris, 1971, vol. 3, pp. 211-215.

[17] K. Grey, ‘‘Further results on designs carried by a code’’, Ars Comb., **26 B** (1988), 133-152.

[18] M. Hall, Jr., ‘‘Hadamard matrices of order 16’’, Jet Propulsion Lab. Research Summary 36-10, Pasadena CA, Vol. 1 (Sept. 1, 1961), pp. 21-26.

[19] M. Hall, Jr., ‘‘Combinatorial Theory’’, Wiley, NY, 2nd ed., 1986.

[20] M. Klemm, ‘‘Ueber die Identität von MacWilliams für die Gewichtsfunktion von Codes’’, Arch. Math., **49** (1987), 400-406.

[21] M. Klemm, ‘‘Selbstduale Codes über dem Ring der ganzen Zahlen modulo 4’’, Arch. Math., **53** (1989), 201-207.

[22] J. S. Leon, V. Pless and N. J. A. Sloane, ‘‘Self-dual codes over $GF(5)$’’, J. Combinatorial Theory, Series A, **32** (1982), pp. 178-194.

[23] F. J. MacWilliams, C. L. Mallows and N. J. A. Sloane, ‘‘Generalizations of Gleason’s theorem on weight enumerators of self-dual codes’’, IEEE Trans. Information Theory, **18** (1972), 794-805.

[24] F. J. MacWilliams and N. J. A. Sloane, ‘‘The Theory of Error-Correcting Codes’’, North-Holland, Amsterdam, 1977.

[25] H. K. Nandi, ‘‘A further note on nonisomorphic solutions of incomplete block designs’’, Sankya, **7** (1945-46), 313-316.

[26] P. Piret, ‘‘Bounds for codes over the unit circle’’, IEEE Trans. Information Theory, **32** (1986), 760-767.

[27] N. J. A. Sloane, ‘‘Error-correcting codes and invariant theory: new applications of a nineteenth-century technique’’, Amer. Math. Monthly, **84** (1977), 82-107.

[28] N. J. A. Sloane, ‘‘Self-dual codes and lattices’’, in *Relations Between Combinatorics and Other Parts of Mathematics*, Proc. Symp. Pure Math. **35**, Amer. Math. Soc., Providence RI, 1979 pp. 273-308.

[29] J. A. Todd, ‘‘A combinatorial problem’’, J. Math. Phys., **12** (1933), 321-333.

[30] W. D. Wallis, A. P. Street and J. S. Wallis, ‘‘Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices’’, Lecture Notes in Math. **292**, Springer-Verlag, NY 1972.

[31] S. K. Wasan, ‘‘On codes over Z_m’’, IEEE Trans. Information Theory, **28** (1982), 117-120.

Figure Captions

Figure 1. Indecomposable codes over Z_4 generated by tetrads, ordered by inclusion. An arrow indicates that the lower code can be obtained from the upper code by adjoining a single tetrad. The arrow has a hollow or solid head according as the number of words increases by a factor of 2 or 4. Note that $\$^{O}_{4} > \$^{+}_{4}$. (In these two figures we have used bold letters instead of script letters, and ‘‘⊕’’ has been written as ‘‘∞’’.)

Figure 2. All self-dual codes of length $n \leq 8$. A vertical or sloping line indicates that the upper code can be obtained by shortening the lower code. The indecomposable codes are in boxes, the others in circles. There are no indecomposable codes of length 9, so that the codes of length 9 are obtainable by adjoining $!_{1}$ to the codes of length 8.