JOURNAL OF COMBINATORIAL THEORY, Series A 32, 178–194 (1982)

Self-Dual Codes over $GF(5)$

J. S. LEON* AND V. PLESS*

Mathematics Department, University of Illinois at Chicago Circle, Box 4348, Chicago, Illinois 60680

AND

N. J. A. SLOANE

Mathematics and Statistics Research Center, Bell Laboratories, Murray Hill, New Jersey 07974

Received August 17, 1981

DEDICATED TO PROFESSOR MARSHALL HALL, JR., ON THE OCCASION OF HIS RETIREMENT

It is shown that a self-orthogonal code over $GF(5)$ which is generated by words of weight 4 has a decomposition into components belonging to three infinite families: d_n $(n = 4, 5, 6, 7, 8, 10, 12,...)$, e_n $(n = 6, 8, 10,...)$ and F_n $(n = 6, 8, 10,...)$. All maximal self-orthogonal (and self-dual) codes of length $\leqslant 12$ are classified, and a number of interesting codes of greater length are constructed.

I. INTRODUCTION

Self-dual codes of modest length over $GF(2)$, $GF(3)$ and $GF(4)$ have been classified in a series of papers (see [6, 7, 28, 32, 37–39, 41] and the references given there). $GF(4)$ had seemed like a good place to terminate the enumeration, since self-dual codes over these three fields enjoy special properties not shared by other codes (notably the presence of gaps in their weight distributions—see the Gleason–Pierce theorem [41, Theorem 6.1.1]). However, recent work on the construction of even unimodular lattices [8–10, 42] has called for the classification of self-dual codes over other alphabets, for example, the cyclic group of order n. In particular the case $n = 5$ leads to self-dual codes over $GF(5)$, the subject of the present paper. Such codes have

* The work of these authors was supported in part by the National Science Foundation under Grant MCS 79-24986.

0097-3165/82/020178–17$02.00/0

also been studied by Gleason and Pierce (cf. [29, Section 5.3.2]), and furthermore arise in studying certain designs (compare [17]). For example, if there is a projective plane of order 10 the $GF(5)$ span of its incidence matrix extends to a self-dual code [18].

We will show that self-dual codes over $GF(5)$ of minimum weight 2 or 4 have a satisfactory decomposition theory (see Theorems 2 and 3). The total number of codes of a given length is known, and leads to a "mass formula" (Theorem 1). From this we are able to obtain a complete enumeration of the codes of length not exceeding 12—see Theorems 4, 5 and Tables II, III. The enumeration is made easier by our having available a computer program ([27]; see also [24–26]) for finding the automorphism group of a code.

The weight enumerator of any one of the codes (the most useful weight distribution to use being the "Lee weight" distribution) is strongly constrained: it must be invariant under a three-dimensional representation of the icosahedral group. These invariants were already known to Felix Klein [22, 23], and the consequences for coding theory were discovered by Gleason and Pierce (and independently by the third author). The result is given in [29, Section 5.3.2] and [30, p. 621], and in a slightly more convenient form in Theorem 6 below. The corresponding result for Hamming weight enumerators is given in Theorem 7. (It is worth mentioning that precisely the same invariants have recently been studied by Hirzebruch in connection with cusps of the Hilbert modular surface associated with $\mathbb{Q}(\sqrt{5})$—see [19, p. 306]. However, there does not appear to be any connection between this work and ours.)

From Theorem 6 we may obtain an upper bound on the minimum weight of these codes. We also describe a number of good codes of length greater than 12, some of which meet these bounds—see Section III and Table IV.

II. Properties of Codes

From now on a code in this paper means a linear code over $GF(5)$. An $[n, k, d]$ code C has length n, dimension k and minimum nonzero weight d. (For any undefined terms from coding theory see [30].) A code is *self-orthogonal* if $C \subset C^{\perp}$ and *self-dual* if $C = C^{\perp}$. Self-dual codes (over $GF(5)$) exist if and only if the length is even. If a codeword u in a self-orthogonal code C contains i 0's, $j \pm 1$'s and $k \pm 2$'s (so that the weight of u is $j + k$), then $u \cdot u = 0$ implies

$$j \equiv k \pmod 5. \tag{1}$$

So although (by the Gleason–Pierce theorem) we cannot constrain the weights in a self-dual code to be multiples of any constant greater than one, nevertheless Eq. (1) reduces the number of types of codewords that can

occur by a factor of 5. Equation (1) also implies that a codeword in a self-orthogonal code cannot have weight 1 or 3, although all other weights can occur. The Lee weight enumerator of C is

$$\mathbf{L}(x, y, z) = \sum_{u \in C} x^i y^j z^k, \tag{2}$$

and the Hamming weight enumerator is

$$\mathbf{W}(x, y) = \mathbf{L}(x, y, y).$$

The number of codewords of weight r in C, the coefficient of y^r in $\mathbf{W}(x, y)$, will be denoted by A_r.

The *monomial group* $\mathrm{Aut}(C)$ of C consists of all $n \times n$ monomial matrices π (with exactly one entry ± 1 in each row and column and all other entries zero) such that $u\pi \in C$ for all $u \in C$. Two codes C, C' are *equivalent* if there is a monomial matrix π such that $C\pi = C'$. If C is self-orthogonal (or self-dual), so is C' (this would not be true in general if π were allowed to contain ± 1's and ± 2's). Equivalent codes have the same weight enumerators. Our aim is to classify the inequivalent self-dual codes of even length and the maximal self-orthogonal codes of odd length. A complete classification is only possible for modest lengths, and otherwise we are primarily interested in those codes with the highest possible minimum weight for a given length.

It is known [36, 37] that the total number of self-dual codes of even length n is

$$\prod_{i=0}^{n/2-1} (5^i + 1)$$

and the number of maximal self-orthogonal codes of odd length n is

$$\prod_{i=1}^{(n-1)/2} (5^i + 1).$$

These results are most conveniently expressed as follows.

THEOREM 1 (The mass formula). *For n even*

$$\sum_C \frac{1}{\mathrm{Aut}(C)} = \frac{\prod_{i=0}^{n/2-1}(5^i + 1)}{2^n \cdot n!}, \tag{3}$$

where the sum is over all inequivalent self-dual codes of length n, and for n odd

$$\sum_C \frac{1}{\mathrm{Aut}(C)} = \frac{\prod_{i=1}^{(n-1)/2}(5^i + 1)}{2^n \cdot n!} \tag{4}$$

TABLE I

Mass of Self-Dual Codes of Length n

n	Mass
2	$\frac{1}{4}$
4	$\frac{1}{32}$
6	$\frac{13}{1920}$
8	$\frac{39}{10240}$
10	$\frac{4069}{614400}$
12	$\frac{2119949}{54067200}$

when the sum is over all inequivalent maximal self-orthogonal codes of length n.

The first few values of the mass (3) are given in Table I.

III. A List of Codes

This section contains a list of the most interesting codes we have found. Those described by upper case letters are self-dual, the others self-orthogonal. The subscript gives the length, and the codes are arranged alphabetically. Minus signs are indicated by bars, so the elements of $GF(5)$ are $\{0, 1, 2, \bar{2}, \bar{1}\}$. The order of the monomial group of a code is denoted by g, and where individual monomials are specified we assume the coordinate positions have been labeled $1, 2, \ldots, n$, and if there is an obvious division of the coordinates into blocks they are labeled $I, II, III, \ldots$. A typical monomial is $(2354) \cdot \bar{3}\bar{4}$, which means that first the permutation (2354) is applied to the coordinates and then coordinates 3 and 4 are negated. As usual in this work we will decompose codes into "components" held together by "glue." This "glueing theory" has been adequately described in earlier papers—see [6, 7].

C_2 is the $[2, 1, 2]$ code consisting of the codewords $\{00, 12, 2\bar{1}, \bar{2}1, \overline{12}\}$. It has generator matrix $[12]$, weight enumerator

$$\alpha = x^2 + 4yz, \tag{5}$$

and its monomial group has order $g = 4$.

d_n (for $n = 4, 6, 8,...$) is the $[n, (n-2)/2, 4]$ code with generator matrix shown in Fig. 1a. For this code $A_4 = 2n - 4$, and $\mathrm{Aut}(d_n)$ is generated by the monomials

$$(2i-1, 2i) \cdot \overline{2i+1}\ \overline{2i+2}\ \overline{2i+3}..., \qquad \text{for} \quad i = 1, 2,..., n/2,$$
$$(1, n)(2, n-1)(3, n-2)... \cdot \bar{2}\bar{4}\bar{6}...,$$

and of course the overall multiplication by -1:

$$\bar{1}\bar{2}\bar{3}\bar{4}...$$

which in the future we shall take for granted. Thus $g = 2^{(n+4)/2}$. There is a two-dimensional glue space spanned by $a = (1100...0)$ and $b = (00...01\bar{1})$.

d_5 is the $[5, 2, 4]$ code with generator matrix

$$\begin{bmatrix} 0 & 2 & 1 & 1 & 2 \\ \bar{2} & 0 & 2 & 1 & 1 \end{bmatrix}.$$

For this code $A_4 = 20$, and $\mathrm{Aut}(d_5)$ is generated by $(12345) \cdot \bar{1}$ and

(a) d_n:
$$\begin{bmatrix} 1 & \bar{1} & 2 & 2 & & & & & \\ & & 1 & \bar{1} & 2 & 2 & & & \\ & & & & 1 & \bar{1} & 2 & 2 & \\ & & & & & & \cdot & \cdot & \cdot \\ & & & & & & 1 & \bar{1} & 2 & 2 \end{bmatrix} \quad (n=4, 6, 8, \cdots)$$

(b) e_n:
$$\begin{bmatrix} 1 & 2 & 1 & 2 & & & & & \\ & & 1 & 2 & 1 & 2 & & & \\ & & & & 1 & 2 & 1 & 2 & \\ & & & & & & \cdot & \cdot & \cdot \\ & & & & & & 1 & 2 & 1 & 2 \end{bmatrix} \quad (n=6, 8, 10, \cdots)$$

(c) F_n:
$$\begin{bmatrix} 1 & \bar{1} & 2 & 2 & & & & & \\ & & 1 & \bar{1} & 2 & 2 & & & \\ & & & & 1 & \bar{1} & 2 & 2 & \\ & & & & & & \cdot & \cdot & \cdot \\ & & & & & & 1 & \bar{1} & 2 & 2 \\ 2 & 2 & & & & & & & 1 & \bar{1} \end{bmatrix} \quad (n=6, 8, 10, \cdots)$$

FIG. 1. Generator matrices for the codes d_n, e_n and F_n.

$(2354) \cdot \bar{3}\bar{4}$, and has order $g = 40$. There is one dimension of glue, generated by $a = (00121)$.

d_7 is the $[7, 3, 4]$ code with generator matrix

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

$A_4 = 24$, $g = 48$, and the glue is generated by $a = (00001\bar{1}\bar{2})$.

e_n (for $n = 6, 8, 10, \ldots$) is the $[n, (n-2)/2, 4]$ code with generator matrix shown in Fig. 1b. Here $A_4 = n(n-2)/2$, $\mathrm{Aut}(e_n)$ is generated by $(12)(34)\ldots \cdot \bar{2}\bar{4}\ldots$, $(I, II) \cdot \bar{I}\,\bar{II}$, etc., and $g = 4(n/2)!$ The glue space is spanned by $a = (010\bar{1}010\bar{1}\ldots)$ and $b = (12000\ldots)$.

F_n (for $n = 6, 8, 10, \ldots$) is the $[n, n/2, 4]$ code with generator matrix shown in Fig. 1c. For $n \geqslant 10$, $A_4 = 2n$ and $\mathrm{Aut}(F_n)$ is generated by $(12)(34) \cdot \bar{3}\bar{4}$, $(34)(56) \cdot \bar{5}\bar{6}$, etc., $(I, II, III, \ldots)$ and $(1, n)(2, n-1)\ldots \cdot \bar{2}\bar{4}\bar{6}\ldots$, and $g = n2^{n/2}$. The codes F_6 and F_8 are exceptional. For F_6 it is more convenient to use the generator matrix

$$\begin{bmatrix} 1 & 0 & 1 & \bar{1} & \bar{1} & 1 \\ 1 & 1 & 0 & 1 & \bar{1} & \bar{1} \\ 1 & \bar{1} & 1 & 0 & 1 & \bar{1} \end{bmatrix}.$$

If we label the coordinates $\infty, 0, 1, 2, 3, 4$ then $\mathrm{Aut}(F_6)$ is generated by $z \to z + 1$; $z \to -1/z$ followed by $\bar{2}, \bar{3}$; and $z \to 2z$ followed by $\bar{\infty}$. Thus $\mathrm{Aut}(F_6) \cong 2 \cdot PGL_2(5)$, of order $g = 240$. Also $A_4 = 60$. This is the "glue code" associated with the Niemeier lattice of type A_4^6—see [8–10, 42]. The weight enumerator of F_6 is

$$\beta' = x^6 + 12x(y^5 + z^5) + 60x^2y^2z^2 + 40y^3z^3, \tag{6}$$

although the polynomial

$$\begin{aligned} \beta &= \tfrac{1}{12}(\alpha^3 - \beta') \\ &= x^4yz - x^2y^2z^2 - x(y^5 + z^5) + 2y^3z^3 \end{aligned} \tag{7}$$

is easier to work with (see Theorem 6 below).

For F_8 it is convenient to use the generator matrix $[I_4, H_4]$, where I_n denotes an $n \times n$ identity matrix and

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \bar{1} & 1 & \bar{1} \\ 1 & 1 & \bar{1} & \bar{1} \\ 1 & \bar{1} & \bar{1} & 1 \end{bmatrix} \tag{8}$$

is a Hadamard matrix. Then $\mathrm{Aut}(F_8)$ has order $2^7 \cdot 3$, being generated by $(I, II) \cdot \overline{II}$ and the automorphism group of H_4 itself, which has order $2^5 \cdot 3$ (cf. [15, 16, 21]). The Lee weight enumerator of F_8 is

$$\delta = x^8 + 48x^4y^2z^2 + 16x^3(y^5 + z^5) + 288x^2y^3z^3 + 64x(y^6z + yz^6) + 128y^4z^4. \tag{9}$$

K_{12} is a $[12, 6, 5]$ code with generator matrix

∞	0	1	2	3	4	∞'	$0'$	$1'$	$2'$	$3'$	$4'$
0	1	1	1	1	1	0	0	0	0	0	0
0	0	0	0	0	0	0	1	1	1	1	1
1	0	1	0	0	$\bar{1}$	0	0	0	$\bar{1}$	1	0
1	$\bar{1}$	0	1	0	0	0	0	0	0	$\bar{1}$	1
1	0	$\bar{1}$	0	1	0	0	1	0	0	0	$\bar{1}$
0	0	0	1	$\bar{1}$	0	1	0	1	0	0	$\bar{1}$

;

and $A_5 = 48$, $g = 480$. The 12 projectively distinct codewords of weight 5 may be regarded as the circuits around each of the 12 vertices of an icosahedron. K_{12} is the first code we have encountered which has minimum weight 5 and is generated by vectors of weight 5. The smallest code of this type is the trivial code

$$k_5\colon [11111].$$

There are infinitely many others, and we have not attempted to classify them. However, it is amusing to note that any two of the generators of such a code overlap in 0 or 2 coordinates, and therefore when regarded as *binary* vectors form an orthonormal set of vectors in $GF(2)^n$.

The next three families of codes, L_n, Q_n and Q_n', are generated by various matrices related to Hadamard matrices.

The Hadamard codes L_n. There are three obvious classes of self-dual codes that can be obtained from Hadamard matrices. Let H_t denote an arbitrary Hadamard matrix of order t. (i) For $n \equiv 0 \pmod{20}$ let L_n be the code generated by the rows of H_n. (ii) For $n \equiv 8 \pmod{40}$ let L_n be the code with generator matrix $[I_{n/2}, H_{n/2}]$. (iii) For $n \equiv 32 \pmod{40}$ let L_n have generator matrix $[2I_{n/2}, H_{n/2}]$. For example, there is a unique code L_8, which is equivalent to F_8.

An upper bound on the minimum weight of any of these codes is obtained from the observation that the sum of any two rows of H_t has weight $t/2$. Furthermore if either the row or column character [20] of H_t exceeds one then there are four rows or columns whose sum has weight $t/4$. Let us consider the codes L_{48} that are obtained from the 59 inequivalent Hadamard matrices of order 24 (see [20]). All these Hadamard matrices except the Paley matrix have either row or column character greater than one, so the corresponding codes have $d \leqslant 10$. In fact one can show by a straightforward analysis that $d = 10$ for these 58 codes. The upper bound for the code obtained from the Paley matrix is $d \leqslant 14$, and we found by computer that $d = 14$. Thus there is a single code L_{48} with parameters [48, 24, 14]. There are many codes of type $L_{20}, L_{32}, L_{40}, \ldots$ (see [12–14]).

The quadratic residue codes Q_n and Q_n' differ from the Hadamard codes only in that the diagonal entries of the Hadamard matrices have been changed. (i) When $n \equiv 0$ or 12 (mod 20) and $n - 1 = q$ is a prime power, let Q_n be the code with generator matrix (m_{ij}), where the rows and columns are labeled $\infty, 0, 1, \ldots, q-1$, and $m_{ii} = \sqrt{-q}$ for all i, $m_{\infty i} = 1$ and $m_{i\infty} = -1$ for $i \geqslant 0$, $m_{ij} = 1$ if $j - i$ is a square in $GF(q)$, and $m_{ij} = -1$ if $j - i$ is a nonsquare $(i, j \geqslant 0,\ i \neq j)$. Then Q_n is the usual self-dual extended quadratic residue code (cf. [2, 30]). The first four of these codes are $Q_{12} = [12, 6, 6]$, $Q_{20} = [20, 10, 8]$, $Q_{32} = [32, 16, 10]$ and $Q_{60} = [60, 30, d \leqslant 18]$ (these minimum weights were found by Newhart [35]). We computed the weight enumerators of Q_{12} and Q_{20}, which are given in Eqs. (15) and (17) in Section V. Q_{12} is the smallest self-dual code of minimum weight 6. Assuming the classification of finite simple groups, $\mathrm{Aut}(Q_n) \cong 2 \cdot PSL_2(q)$ (see [1; 5; 30, p. 494; 40]).

(ii) A conference matrix B_n is a real $n \times n$ matrix with diagonal entries 0 and other entries ± 1 which satisfies $B_n B_n^{tr} = (n-1) I_n$—see [11]. For $n \equiv 6$ (mod 10) let Q_n be the self-dual code generated by the rows of a conference matrix B_n, if one exists. For example, $Q_6 \cong F_6$. A more interesting example is obtained from Williamson's construction [43] of a B_{16}, which gives a [16, 8, 7] code Q_{16} with generator matrix

$$\begin{bmatrix} B_4 & H_4 & H_4 & H_4 \\ \bar{H}_4 & B_4 & H_4 & \bar{H}_4 \end{bmatrix},$$

where H_4 is given in (8) and

$$B_4 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ \bar{1} & 0 & 1 & \bar{1} \\ \bar{1} & \bar{1} & 0 & 1 \\ \bar{1} & 1 & \bar{1} & 0 \end{bmatrix}.$$

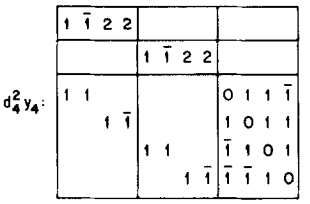

FIG. 2. Generator matrix for the code $d_4^2 y_4$.

(iii) For $n \equiv 12 \pmod{20}$ let Q_n' be the code generated by the rows of $B_n + 2I_n$, where B_n is a skew-symmetric conference matrix. (iv) For $n \equiv 0 \pmod{20}$ let Q_n' be generated by $[I_{n/2}, B_{n/2}]$, where $B_{n/2}$ is any conference matrix. For example, we found by computer that the Paley matrix B_{20} produces a $[40, 20, 13]$ code Q_{40}'. (v) For $n \equiv 32 \pmod{40}$ let Q_n'' be generated by $[I_{n/2}, B_{n/2} + 2I_{n/2}]$, where $B_{n/2}$ is skew-symmetric. (vi) For $n \equiv 4 \pmod{20}$ let Q_n be generated by $[2I_{n/2}, B_{n/2}]$, where $B_{n/2}$ is any conference matrix. For example, we found by computer that the Paley matrix B_{12} produces a $[24, 12, 9]$ code Q_{24}. (vii) Finally for $n \equiv 16 \pmod{40}$ let Q_n' be generated by $[2I_{n/2}, B_{n/2} + 2I_{n/2}]$, where $B_{n/2}$ is skew-symmetric.

R_{14} is a $[14, 7, 6]$ code with generator matrix

$$\begin{bmatrix}
\bar{1} & 2 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\bar{1} & \bar{1} & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\bar{2} & \bar{2} & 2 & 0 & \bar{1} & 2 & \bar{1} & 1 & 1 & \bar{1} & \bar{1} & \bar{1} & 1 & \bar{1} \\
0 & 0 & \bar{1} & \bar{1} & 2 & 1 & \bar{1} & 1 & 1 & 1 & \bar{1} & \bar{1} & \bar{1} & 1 \\
\bar{2} & \bar{2} & 2 & \bar{1} & 2 & 0 & \bar{1} & \bar{1} & 1 & 1 & 1 & \bar{1} & \bar{1} & \bar{1} \\
0 & 0 & \bar{1} & \bar{1} & 1 & \bar{1} & 2 & 1 & \bar{1} & 1 & 1 & 1 & \bar{1} & \bar{1} \\
\bar{2} & \bar{2} & 2 & 2 & 2 & \bar{1} & 2 & 2 & 1 & \bar{1} & 1 & 1 & 1 & \bar{1}
\end{bmatrix},$$

and $A_6 = 252$.

Finally y_n denotes the "empty component" of length n. An example is given in Fig. 2 (see [6, 7] for more details).

IV. CLASSIFICATION

The codes with minimum weight 2 can be easily disposed of.

THEOREM 2. *If C is self-orthogonal of length >2 and has minimum weight 2 then $C = C_2 \oplus C'$ for some self-orthogonal code C'.*

Proof. Without loss of generality C contains the vector $u = 1200...0$. Any vector orthogonal to u must begin 12... or 00..., and the result follows. Q.E.D.

Suppose now that C has minimum weight 4. Let C' be the subcode of C generated by words of weight 4. Then C' is described by the following theorem.

THEOREM 3. *A self-orthogonal code of minimum weight* 4 *which is generated by words of weight* 4 *is a direct sum of components taken from the list* $d_4, d_5, d_6, d_7, d_8, d_{10}, d_{12}, ..., e_6, e_8, e_{10}, ..., F_6, F_8, F_{10}, ...$.

The proof is postponed until the end of this section. We now examine how these codes can be combined to produce self-dual codes.

THEOREM 4. *The only self-dual codes of length* $\leqslant 12$ *are those shown in Tables* II *and* III.

In these tables the letters i and d indicate whether the code is indecomposable or decomposable. The fourth column gives the minimum weight, and the fifth column either the weight enumerator or the number of words of minimum weight. The glue vectors are described in the notation of Section III. For example, the glue vector for the code $d_5 d_7$ is

$$(a, 2a) = (00121, 00002\bar{2}1).$$

The glue for the code $d_4^2 y_4$ is given in Fig. 2.

TABLE II

Self-Dual Codes of Length $\leqslant 10$

Length	Components	Type	d	Wt. Dbn.	Glue	Group
2	C_2	i	2	α	—	4
4	C_2^2	d	2	α^2	—	$2 \cdot 4^2$
6	C_2^3	d	2	α^3	—	$3! \cdot 4^3$
6	F_6	i	4	β'	—	$2 \cdot PGL_2(5)$
8	C_2^4	d	2	α^4	—	$4! \cdot 4^4$
8	$C_2 F_6$	d	2	$\alpha\beta'$	—	$4 \cdot 240$
8	F_8	i	4	δ	—	$2^7 \cdot 3$
10	C_2^5	d	2	α^5	—	$5! \cdot 4^5$
10	$C_2^2 F_6$	d	2	$\alpha^2\beta'$	—	$32 \cdot 240$
10	$C_2 F_8$	d	2	$\alpha\delta$	—	$4 \cdot 384$
10	F_{10}	i	4	$\alpha^5 - 20\alpha^2\beta$	—	$2^6 \cdot 5$
10	e_{10}	i	4	$\alpha^5 - 20\alpha^2\beta - 4\gamma$	a	$2^5 \cdot 3 \cdot 5$
10	d_5^2	i	4	$\alpha^5 - 20\alpha^2\beta - 4\gamma$	$(a, 2a)$	$2^6 \cdot 5^2$

TABLE III

Self-Dual Codes of Length 12

Length	Components	Type	d	Wt. Dbn.	Glue	Group
12	C_2^6	d	2	α^6	—	$6! \cdot 4^6$
12	$C_2^3 F_6$	d	2	$\alpha^3\beta'$	—	$3!4^3 \cdot 240$
12	$C_2^2 F_8$	d	2	$\alpha^2\delta$	—	$32 \cdot 384$
12	$C_2 F_{10}$	d	2	$A_2 = 4$	—	$4 \cdot 320$
12	$C_2 e_{10}$	d	2	$A_2 = 4$	$(0, a)$	$4 \cdot 480$
12	$C_2 d_5^2$	d	2	$A_2 = 4$	$(0, a, 2a)$	$4 \cdot 1600$
12	F_6^2	d	4	$(\beta')^2$	—	$2 \cdot 240^2$
12	e_{12}	i	4	$A_4 = 60$	$a + b$	$2^6 \cdot 3^2 \cdot 5$
12	$d_5 d_7$	i	4	$A_4 = 44$	$(a, 2a)$	$2^6 \cdot 3 \cdot 5$
12	F_{12}	i	4	$A_4 = 24$	—	$2^8 \cdot 3$
12	e_6^2	i	4	$A_4 = 24$	$(a, 2a), (2\bar{b}, 2\bar{a} + \bar{b})$	$2^5 \cdot 3^2$
12	$d_6 e_6$	i	4	$A_4 = 20$	$(a + 2b, b), (b, 2\bar{a} + 2\bar{b})$	$2^5 \cdot 3$
12	d_4^3	i	4	$A_4 = 12$	$(0, 2\bar{a} + 2\bar{b}, a + b)_{\text{cycle}}$	$2^7 \cdot 3$
12	$d_4^2 y_4$	i	4	$A_4 = 8$	See Fig. 2	2^6
12	K_{12}	i	5	$A_5 = 48$	—	$2^5 \cdot 3 \cdot 5$
12	Q_{12}	i	6	Eq. (15)	—	$2 \cdot PSL_2(11)$

Proof of Theorem 4. There are three steps in the proof. First we determine the group of each code, using the computer [27] where necessary. Second, we check that all the codes shown are inequivalent. Third, we verify that the sum of the reciprocals of the group orders for the codes of each length is equal to the mass given in Table I. Q.E.D.

Remark. Although the list of codes is self-explanatory, it is worth mentioning that some of these codes were initially found by applying a *transvection* to a known code C. We choose a vector $a \notin C$ and define the transvection

$$\tau_a : x \to x - (x \cdot a)a.$$

Then, provided $a \cdot a = 2$, the new code

$$C' = \{\tau_a(x), x \in C\}$$

is a self-dual code which intersects C in a subcode of codimension 1. Two of the codes of length 12 were initially found by applying this technique with $C = Q_{12}$, and R_{14} was obtained similarly from $C_2 \oplus Q_{12}$.

Using Theorem 4 we can classify the maximal self-orthogonal codes of odd length, having parameters $[n, (n-1)/2, d]$ for some d, for all lengths $\leqslant 11$. These occur as "children" of the self-dual codes of length $n+1$, as described in [6, 39]. For example, the $d_5 d_7$ code has two self-orthogonal

children of length 11. If one of the first five coordinates is set to zero a $d_4 d_7$ code is obtained, while setting one of the last seven coordinates to zero produces a $d_5 d_6$. The number of children that a code C possesses is the number of orbits of $\mathrm{Aut}(C)$ on the coordinates. For all but one of the codes of Tables II and III this number is easily found. The surprise is $d_6 e_6$, for which the group has three orbits, $\{1, 2, 5, 6\}$, $\{3, 4\}$, $\{7, 8, \ldots, 12\}$, giving rise to the three children $d_4 e_6 y_1$, $e_6 k_5$ and $d_4 d_6 y_1$. A second (and inequivalent) $d_4 e_6 y_1$ code arises as a child of e_6^2. In the following theorem only the components of the children are given, as the glue vectors can be easily recovered from the parents. One new component is needed for this theorem: z_1 is the zero code of length 1—a code containing a component z_1 has a coordinate position in which every codeword is zero.

THEOREM 5. *The following list gives all maximal self-orthogonal codes of lengths* 1, 3,..., 11:

length 1: z_1.

length 3: $C_2 z_1$.

length 5: $C_2^2 z_1, d_5$.

length 7: $C_2^3 z_1, C_2 d_5, F_6 z_1, d_7$.

length 9: $C_2^4 z_1, C_2^2 d_5, C_2 F_6 z_1, C_2 d_7, F_8 z_1, d_8 y_1, e_8 y_1, d_4 d_5$.

length 11: $C_2^5 z_1, C_2^3 d_5, C_2^2 F_6 z_1, C_2^2 d_7, C_2 F_8 z_1, C_2 d_8 y_1, C_2 e_8 y_1, C_2 d_4 d_5, F_{10} z_1, e_{10} z_1, d_5^2 z_1, F_6 d_5, e_{10} y_1, d_4 d_7, d_5 d_6, d_{10} y_1, d_4 e_6 y_1$ (*two inequivalent codes*), $e_6 k_5, d_4 d_6 y_1, d_4^2 y_3$ (*two inequivalent codes*), $d_4 y_7, K_{11}, Q_{11}$,

where $K_{11} = [11, 5, 5]$ *and* $Q_{11} = [11, 5, 6]$ *are obtained by setting any coordinate of* K_{12} *and* Q_{12}, *respectively, to zero.*

Proof of Theorem 3. Let C be an indecomposable self-orthogonal $[n, k, 4]$ code which is spanned by vectors of weight 4. The proof is by induction on k. If $k = 1$ there is a unique code which we may take to be d_4. Two codewords in C of weight 4 may overlap only in 0, 2 or 3 coordinates. If $k = 2$ there are three possibilities for C,

$$\begin{pmatrix} 1 & \bar{1} & 2 & 2 & 0 \\ 0 & 1 & 1 & 2 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & \bar{1} & 2 & 2 & 0 & 0 \\ 0 & 0 & 1 & \bar{1} & 2 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 & 2 \end{pmatrix},$$

which are equivalent to d_5, d_6 and e_6, respectively (d_6 and e_6 have different values of A_4 so they are inequivalent). If $k = 3$ it is clear that $6 \leqslant n \leqslant 8$. If C is an $[8, 3, 4]$ code there cannot be much overlap among the generators, and we find there are just two possibilities, d_8 and e_8. If C is a $[7, 3, 4]$ code then $C \cong d_7$ from Theorem 5. If C is a $[6, 3, 4]$ code then $C \cong F_6$ from Theorem 4.

Finally suppose $k \geqslant 4$ and let C' be an $[n, k-1, 4]$ subcode of C. We obtain C from C' by adjoining a glue vector of C' (see Section III) which is a self-orthogonal vector of weight 4. There are only three ways in which this can be done, leading to the codes d_n, e_n and F_n (for n even $\geqslant 6$). Q.E.D.

V. Weight Distributions

Let C be a self-dual code of length n with Lee weight enumerator $\mathbf{L}(x, y, z)$ and Hamming weight enumerator $\mathbf{W}(x, y) = \mathbf{L}(x, y, y)$. Then it is known (see [29, Section 5.3.2]) that $\mathbf{L}(x, y, z)$ is invariant under the icosahedral group of order 120 (the group $[3, 5]$ in Coxeter's notation), and therefore that the following theorem holds (cf. [22, 23, 29]).

Theorem 6 (Klein, Gleason and Pierce). *The Lee weight enumerator of a self-dual code is a polynomial in α, β, and γ, where α and β are defined in* (5) *and* (7), *and*

$$\begin{aligned}\gamma = {} & 5x^6y^2z^2 - 4x^5(y^5 + z^5) - 10x^4y^3z^3 \\ & + 10x^3(y^6z + yz^6) + 5x^2y^4z^4 - 10x(y^7z^2 + y^2z^7) \\ & + 6y^5z^5 + y^{10} + z^{10}. \end{aligned} \tag{10}$$

For example, the weight enumerators of C_2 and F_6 are, respectively, α and $\beta' = \alpha^3 - 12\beta$ (see also Table II). The polynomials α, β and γ are algebraically independent. But when we set $y = z$, α, β and γ become

$$\bar{\alpha} = x^2 + 4y^2, \tag{11}$$

$$\begin{aligned}\bar{\beta} &= x^4y^2 - x^2y^4 - 2xy^5 + 2y^6 \\ &= y^2(x-y)^2(x^2 + 2xy + 2y^2), \end{aligned} \tag{12}$$

$$\begin{aligned}\bar{\gamma} &= y^4(x-y)^4(5x^2 + 12xy + 8y^2) \\ &= 5x^6y^4 - 8x^5y^5 - 10x^4y^6 + 20x^3y^7 \\ &\quad + 5x^2y^8 - 20xy^9 + 8y^{10}, \end{aligned} \tag{13}$$

respectively, which are no longer independent but are related by the syzygy

$$\begin{aligned}16\bar{\gamma}^3 + (\bar{\alpha}^3 - 40\bar{\beta})\,\bar{\alpha}^2\bar{\gamma}^2 - 10(\bar{\alpha}^3 - 36\bar{\beta})\,\bar{\alpha}\bar{\beta}^2\gamma \\ + \bar{\beta}^4(25\bar{\alpha}^3 - 864\bar{\beta}) = 0. \end{aligned} \tag{14}$$

From this we deduce the following theorem.

THEOREM 7. *The Hamming weight enumerator of a self-dual code is an element of the ring*

$$\mathbb{C}[\bar{\alpha}, \bar{\beta}] \oplus \bar{\gamma}\mathbb{C}[\bar{\alpha}, \bar{\beta}] \oplus \bar{\gamma}^2\mathbb{C}[\bar{\alpha}, \bar{\beta}].$$

(The history of Theorem 7 is uncertain. We heard it from Nick Patterson in 1980, but it is probably much older.)

Let us consider the highest minimum weight that is permitted by Theorem 6, i.e., the *extremal weight enumerator* as defined in [31, 33]. For example, at length 12 Theorem 6 implies that $\mathbf{L}(x, y, z)$ is a linear combination of α^6, $\alpha^3\beta$, β^2 and $\alpha\gamma$. The combination with the highest minimum weight, the extremal weight enumerator, is

$$\begin{aligned}\alpha^6 - 24\alpha^3\beta - 6\beta^2 + 6\alpha\gamma \\ = x^{12} + 440x^6y^3z^3 + 264x^5(y^6z + yz^6) + 2640x^4y^4z^4 \\ + 1320x^3(y^7z^2 + y^2z^7) + 5544x^2y^5z^5 + 1320x(y^8z^3 + y^3z^8) \\ + 24(y^{11}z + yz^{11}) + 1144y^6z^6. \qquad (15)\end{aligned}$$

This polynomial has nonnegative integer coefficients, and so could be the weight enumerator of a code of minimum weight 6. In this case such a code does exist, namely, Q_{12}. A similar calculation can be performed for any length n. The number a_n of linearly independent invariants of degree n is the coefficient of λ^n in the Taylor series expansion of

$$\frac{1}{(1-\lambda^2)(1-\lambda^6)(1-\lambda^{10})}, \qquad (16)$$

which for small n is given by

n:	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32
a_n:	1	1	1	2	2	3	4	4	5	6	7	8	9	10	11	13	14.

(It is not difficult to write down an explicit expression for a_n, which grows like $n^2/120$ for large n.)

If nothing goes wrong, the extremal weight enumerator has minimum weight $a_n + 2$ for $n \geqslant 6$. There are three things that can go wrong: the extremal weight enumerator may contain a negative or nonintegral coefficient, it may not be possible to force all the coefficients of terms of weight $\leqslant a_n + 1$ to vanish simultaneously, or all the coefficients of the terms of

TABLE IV

Highest Possible Minimum Weight of a Self-Dual Code

Length	$d_{\max}$	Code	Length	$d_{\max}$	Code
2	2	C_2	14	6	R_{14}
4	2	C_2^2	16	7	Q_{16}
6	4	F_6	18	$\leqslant 8$	?
8	4	F_8	20	8	Q_{20}
10	4	F_{10}	22	$\leqslant 9$	?
12	6	Q_{12}	24	9 or 10	?

weight $a_n + 2$ may accidentally vanish. The corresponding problem for binary self-dual codes has been studied in [31, 33], but since the bound that would be obtained here would be so weak (a quadratic in n), and since one of the first two things already goes wrong at lengths 10, 20, 22 and 24, we have not attempted to prove a general result. At length 20, for example, $d = 9$ is unattainable, and the highest minimum weight we can hope for is $d = 8$. In fact the quadratic residue code Q_{20} (see Section III) has minimum weight 8, and its weight enumerator is

$$\begin{aligned}\alpha^{10} - 40\alpha^7\beta + 310\alpha^4\beta^2 - 270\alpha\beta^3 + 10\alpha^5\gamma - 50\alpha^2\beta\gamma + 40\gamma^2 \\ = x^{20} + 2280x^{12}y^4z^4 + \cdots \\ + 100{,}016y^{10}z^{10} + 9120(y^{15}z^5 + y^5z^{15}) + 40(x^{20} + y^{20}). \quad (17)\end{aligned}$$

The results obtained by examining the extremal weight enumerators are collected in Table IV, which gives for each length n the highest attainable d and an example of a code meeting this bound when one is known. For length 24 the code Q_{24} has $d = 9$, and the extremal weight enumerator shows that $d = 11$ is impossible.

We conclude with some open questions. Do [18, 9, 8], [22, 11, 9], [24, 12,10],... codes exist (see Table IV)? Find other general constructions for self-dual codes. If C is a maximal self-orthogonal code of odd length, how are the Lee weight enumerators of C and $C^\perp$ related?

ACKNOWLEDGMENTS

We should like to thank A. R. Calderbank, J. H. Conway and W. M. Kantor for some helpful discussions. The computations were performed using ALTRAN [4], CAMAC [3], FORTRAN, MACSYMA [34] and PL/1, and we thank the Computer Centers of the University of Illinois at Chicago Circle, Bell Laboratories at Murray Hill, and the M.I.T. Laboratory for Computer Science for their assistance.

REFERENCES

1. E. F. ASSMUS, JR. AND H. F. MATTSON, JR., New 5-designs, *J. Combin. Theory* **6** (1969), 122–151.
2. E. F. ASSMUS, JR. AND H. F. MATTSON, JR., On weights in quadratic-residue codes, *Discrete Math.* **3** (1972), 1–20.
3. D. BERGSTRAND AND T. GRACE, "CAMAC User's Manual," University of Illinois at Chicago Circle, Chicago, 1981.
4. W. S. BROWN, "ALTRAN User's Manual," 4th ed., Bell Laboratories, Murray Hill, N.J., 1977.
5. P. J. CAMERON, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981), 1–22.
6. J. H. CONWAY AND V. PLESS, On the enumeration of self-dual codes, *J. Combin. Theory Ser. A* **28** (1980), 26–53.
7. 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. Inform. Theory* **IT-25** (1979), 312–322.
8. J. H. CONWAY AND N. J. A. SLOANE, On the enumeration of lattices of determinant one, *J. Number Theory*, in press.
9. J. H. CONWAY, R. A. PARKER, AND N. J. A. SLOANE, The covering radius of the Leech lattice, *Proc. Roy. Soc.*, in press.
10. J. H. CONWAY AND N. J. A. SLOANE, Twenty-three constructions for the Leech lattice, *Proc. Roy. Soc.*, in press.
11. J. M. GOETHALS AND J. J. SEIDEL, Orthogonal matrices with zero diagonal, *Canad. J. Math.* **19** (1967), 1001–1010.
12. M. HALL, JR., "Hadamard Matrices of Order 16," Research Summary No. 36-10, Vol. 1, pp. 21–26, Jet Propulsion Lab., Pasadena, Calif., September 1, 1961.
13. M. HALL, JR., "Hadamard Matrices of Order 20," Technical Report 32-761, Jet Propulsion Lab., Pasadena, Calif., November 1, 1965.
14. M. HALL, JR., "Combinatorial Theory," Ginn (Blaisdell), Waltham, Mass., 1967.
15. M. HALL, JR., Automorphisms of Hadamard matrices, *SIAM J. Appl. Math.* **17** (1969), 1094–1101.
16. M. HALL, JR., Semi-automorphisms of Hadamard matrices, *Math. Proc. Cambridge Philos. Soc.* **77** (1975), 459–473.
17. M. HALL, JR., Coding theory of designs, *in* "Finite Geometries and Designs," pp. 134–145, Proceedings, Second Isle of Thorns Conf., London Math. Soc. Lecture Note Series 49, Cambridge Univ. Press, Cambridge, 1981.
18. C. HERING, On codes and projective designs, *Kyoto Univ. Math. Res. Inst. Seminar Notes* **344** (1979), 26–60.
19. F. HIRZEBRUCH, The ring of Hilbert modular forms for real quadratic fields of small discriminant, *in* "Modular Functions of One Variable *VI*," pp. 288–323, Proceedings, Bonn 1976, Lecture Notes in Mathematics No. 627, Springer-Verlag, New York, 1977.
20. N. ITO, J. S. LEON, AND J. Q. LONGYEAR, Classification of 3-(24, 12, 5) designs and 24-dimensional Hadamard matrices, *J. Combin. Theory Ser. A* **31** (1981), 66–93.
21. W. M. KANTOR, Automorphism groups of Hadamard matrices, *J. Combin. Theory* **6** (1969), 279–281.
22. F. KLEIN, Weitere Untersuchunger über das Ikosaeder, *Math. Ann.* **12** (1877) ("Gesammelte Mathematische Abhandlungen," Vol. II, pp. 321–384, Springer-Verlag, New York, 1973).
23. F. KLEIN, "Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree," 2nd ed., Dover, New York, 1956.
24. J. S. LEON, An algorithm for computing the automorphism group of a Hadamard matrix, *J. Combin. Theory Ser. A* **27** (1979), 289–306.

25. J. S. LEON, On an algorithm for finding a base and strong generating set for a group given by generating permutations, *Math. Comp.* **35** (1980), 941–974.
26. J. S. LEON, Finding the order of a permutation group, *in* "The Santa Cruz Conference on Finite Groups," Proc. Sympos. Pure Math. Vol. XXXVII, pp. 511–517, Amer. Math. Soc., Providence, R.I., 1980.
27. J. S. LEON, Computing automorphism groups of error correcting codes, *IEEE Trans. Inform. Theory*, in press.
28. J. S. LEON, V. PLESS, AND N. J. A. SLOANE, On ternary self-dual codes of length 24, *IEEE Trans. Inform. Theory* **IT-27** (1981), 176–180.
29. F. J. MACWILLIAMS, C. L. MALLOWS, AND N. J. A. SLOANE, Generalization of Gleason's theorem on weight enumerators of self-dual codes, *IEEE Trans. Inform. Theory* **IT-18** (1972), 794–805.
30. F. J. MACWILLIAMS AND N. J. A. SLOANE, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.
31. C. L. MALLOWS, A. M. ODLYZKO, AND N. J. A. SLOANE, Upper bounds for modular forms, lattices, and codes, *J. Algebra* **36** (1975), 68–76.
32. C. L. MALLOWS, V. PLESS, AND N. J. A. SLOANE, Self-dual codes over *GF*(3), *SIAM J. Appl. Math.* **31** (1976), 649–666.
33. C. L. MALLOWS AND N. J. A. SLOANE, An upper bound for self-dual codes, *Inform. and Control* **22** (1973), 188–200.
34. MATHLAB GROUP, "MACSYMA Reference Manual," Version 9, Laboratory for Computer Science, MIT Press, Cambridge, Mass., 1977.
35. D. NEWHART, Low weights in extended quadratic residue codes, preprint.
36. V. PLESS, The number of isotropic subspaces in a finite geometry, *Att. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* **39** (1965), 418–421.
37. V. PLESS, On the uniqueness of the Golay codes, *J. Combin. Theory* **5** (1968), 215–228.
38. V. PLESS, A classification of self-orthogonal codes over *GF*(2), *Discrete Math.* **3** (1972), 209–246.
39. V. PLESS, The children of the (32, 16) doubly even codes, *IEEE Trans. Inform. Theory* **IT-24** (1978), 738–746.
40. E. P. SHAUGHNESSY, Codes with simple automorphism groups, *Arch. Math.* **22** (1971), 459–466.
41. N. J. A. SLOANE, Self-dual codes and lattices, *in* "Relations between Combinatorics and Other Parts of Mathematics," Proc. Sympos. Pure Math. Vol. XXXIV, pp. 273–308, Amer. Math. Soc., Providence, R.I., 1979.
42. B. B. VENKOV, On the classification of integral even unimodular 24-dimensional quadratic forms, *Proc. Steklov Inst. Math.*, Issue 4 (1980), 63–74.
43. J. WILLIAMSON, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.* **11** (1944), 65–81.