BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 80, Number 6, November 1974

BINARY SELF-DUAL CODES OF LENGTH 24

BY VERA PLESS[1] AND N. J. A. SLOANE

Communicated by Olga Taussky Todd, February 28, 1974

ABSTRACT. There are 26 distinct indecomposable self-dual codes of length 24 over $GF(2)$, including unique codes of minimum weights 8 and 6, whose groups are, respectively, the Mathieu group M_{24} and the maximal subgroup of index 1771 in M_{24}. For each code we give the order of its group, the number of equivalent codes, and its weight distribution.

1. **Introduction.** An $[n, k]$ code C is a k-dimensional subspace of the vector space of all n-tuples of 0's and 1's with mod 2 addition. The dual code $C^\perp = \{u: u \cdot v = 0$ for all $v \in C\}$ is an $[n, n-k]$ code. C is self-orthogonal if $C \subset C^\perp$, self-dual if $C = C^\perp$. Self-dual codes exist whenever the length n is even. The weight of a vector is the number of its nonzero components, and the minimum weight of C is the minimum weight of any nonzero codeword. The weight distribution of C is the set $\{\alpha_0, \alpha_1, \cdots, \alpha_n\}$, where α_i is the number of codewords of weight i.

The group $\mathcal{G}(C)$ of a code C is the set of all permutations of the coordinates which send C into itself set-wise. Two codes are equivalent if there is a coordinate permutation sending one into the other. The number of codes equivalent to C is $n!/$order of $\mathcal{G}(C)$. The direct sum of codes C' and C'', written $C' \oplus C''$, is $\{(u, v): u \in C', v \in C''\}$. If $C = C' \oplus C''$, where C' and C'' are nonzero, then C is decomposable. Otherwise C is indecomposable.

Pless [4] classified all self-dual codes of length $\leqslant 20$, Conway (unpublished) found the 9 self-dual codes of length 24 in which the weight of every codeword is a multiple of 4, and Niemeier [2] found the 24 even unimodular lattices in dimension 24, 9 of which correspond to the codes found by Conway.

AMS (MOS) subject classifications (1970). Primary 94A10; Secondary 05A15, 15A03.

[1] The work of the first author was supported in part by Project MAC, an MIT interdepartmental laboratory sponsored by the Advanced Research Projects Agency, Department of Defense, under Office of Naval Research Contract N00014–70–A-0362-0001.

We have found that there are 8 inequivalent, indecomposable self-dual codes of length 22, and 26 of length 24. The latter are shown in Table I, which gives for each code a basis, the order of its group, the number of codes equivalent to it (written as a multiple of $\nu = 1 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot 23 = 316,$ $234, 143, 225$), and the weight distribution $\alpha_4, \alpha_6, \cdots, \alpha_{12}$ (omitting $\alpha_0 = 1$, $\alpha_2 = \alpha_{\text{odd}} = 0$, $\alpha_i = \alpha_{24-i}$ for $i > 12$). Full details of the enumeration will appear in [5].

2. **Self-orthogonal codes of minimum weight 4.** Table I was obtained by classifying the codes according to minimum weight. A self-dual code of minimum weight 2 is decomposable. For minimum weight 4 we use

THEOREM 1. *Let C be an indecomposable self-orthogonal code generated by codewords of weight 4. Then C is one of the codes d_n ($n = 4, 6, 8, \cdots$), e_7, or E_8, generated by the rows of the following matrices:*

$$d_n: \underbrace{\begin{bmatrix} 1111 & & & \\ & 1111 & & \\ & & \ddots & \\ & & & 1111 \end{bmatrix}}_{n}, \qquad e_7: \begin{bmatrix} 1111000 \\ 0011110 \\ 1010101 \end{bmatrix}, \qquad E_8: \begin{bmatrix} 11110000 \\ 00111100 \\ 00001111 \\ 10101010 \end{bmatrix}.$$

Furthermore a self-dual code containing E_8 as a subcode is decomposable.

Let C be an indecomposable self-dual code of length 24, and let C' be the subcode generated by codewords of weight 4. By Theorem 1, C' has the form $d_{n_1} \oplus \cdots \oplus d_{n_l} \oplus e_7 \oplus \cdots \oplus e_7$. We considered all such C' and all ways of extending C' to a self-dual code. For each code we computed the order of its group. In this way all the codes of minimum weight 4 were obtained.

The notation used to specify the basis vectors is best illustrated by an example. The code J_{24} generated by the rows of (1)

$$(1) \qquad J_{24}: \left[\begin{array}{c|c|c|c} 11110000 & & & \\ 00111100 & & & \\ 00001111 & & & \\ \hline & 1111000 & & \\ & 0011110 & & \\ & 1010101 & & \\ \hline & & 1111000 & \\ & & 0011110 & \\ & & 1010101 & \\ \hline 11000000 & 1111111 & & 1 \\ 11000000 & & 1111111 & 1 \\ 10101010 & & & 11 \end{array}\right] = \left[\begin{array}{c|c|c|c} d_8 & 0 & 0 & 00 \\ \hline 0 & e_7 & 0 & 00 \\ \hline 0 & 0 & e_7 & 00 \\ \hline b & c & 0 & 10 \\ \hline b & 0 & c & 01 \\ \hline a & 0 & 0 & 11 \end{array}\right]$$

where $a = 101010\ldots10$, $b = 110000\ldots00$, $c = 111\ldots1$, is written $d_8 e_7^2$

$+\ 2/bco10/boc01/ao^2 1^2$, where the $+2$ indicates two coordinates which do not meet any codeword of weight 4. a' denotes $a + b = 011010\ldots10$. We omit the full details of W_{24}, X_{24}, Y_{24}.

3. **Minimum weight 6 and 8.** It is known [3], [1] that the [24, 12] Golay code is the unique code of minimum weight 8, and that its group is the Mathieu group M_{24}.

We determined that there is a unique self-dual code of minimum weight 6, which is generated (in Todd's [6] notation) by the set of 64 nonspecial hexads associated with any set of 6 mutually complementary tetrads in the Golay code. Its group is a maximal subgroup of index 1771 in M_{24}.

TABLE I

Indecomposable Self-Dual Codes of Length 24 (Page 1)

Code	Generator Matrix / Order of Group	Number $\div\ \nu$	α_4	α_6	α_8	α_{10}	α_{12}
A_{24}	$d_{12}^2/ab/ba$ $(2^5 \cdot 6!)^2 \cdot 2$	1,848	30	0	639	0	2756
B_{24}	$d_{10}e_7^2/bcc/aoc$ $2^4 \cdot 5!168^2 \cdot 2$	$18{,}102\frac{6}{7}$	24	0	663	0	2720
C_{24}	$d_8^3(a)/abb/bab/bba$ $(2^3 \cdot 4!)^3 \cdot 3!$	46,200	18	0	687	0	2684
D_{24}	$d_6^4(a)/baao/obaa/aoba/aaob$ $(2^2 \cdot 3!)^4 4!$	246,400	12	0	711	0	2648
E_{24}	d_{24}/a $2^{11} \cdot 12$	2	66	0	495	0	2972
F_{24}	$d_4^6(a)/boa^3o/oboa^3/aoboa^2/a^2oboa/a^3obo/oa^3ob$ $4^6 \cdot 6!3$	221,760	6	0	735	0	2612
G_{24}	Golay code $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	$8{,}013\frac{21}{23}$	0	0	759	0	2576
H_{24}	$d_8 d_{16}/ab/ba$ $2^3 \cdot 4!2^7 \cdot 8!$	1,980	34	64	239	960	1500
I_{24}	$d_4 d_8 d_{12}/b^3/a^2o/oa^2$ $2 \cdot 2!2^3 \cdot 4!2^5 \cdot 6!$	110,880	22	64	287	960	1428

TABLE I

Indecomposable Self-Dual Codes of Length 24 (Page 2)

Code	Generator Matrix Order of Group	Number $\div \nu$	α_4	α_6	α_8	α_{10}	α_{12}
J_{24}	$d_8e_7^2 + 2/bco10/boc01/ao^2 1^2$ (see (1)) $2^3 \cdot 4!168^2 \cdot 2$	$181{,}028\frac{4}{7}$	20	64	295	960	1416
K_{24}	$d_6d_{10}e_7 + 1/b^2c1/oao1/abo1$ $2^2 \cdot 3!2^4 \cdot 5!168$	253,440	20	64	295	960	1416
L_{24}	$d_8^3(b)/b^3/a^2o/oa^2$ $(2^3 \cdot 4!)^3 \cdot 3!$	46,200	18	64	303	960	1404
M_{24}	$d_8^3(c)/a^3/ba'o/boa'$ $(2^3 \cdot 4!)^3 \cdot 2$	138,600	18	64	303	960	1404
N_{24}	$d_6^2d_{10} + 2/b^3 11/oa^2 11/abo01/bao10$ $(2^2 \cdot 3!)^2 2^4 \cdot 5!2$	887,040	16	64	311	960	1392
O_{24}	$d_4^2d_8^2/ab^2o/boao/oboa/baob$ $(2 \cdot 2!)^2(2^3 \cdot 4!)^2 \cdot 2$	1,663,200	14	64	319	960	1380
P_{24}	$d_4d_6^2e_7 + 1/ob^2c1/ab^2o0/oaa'o0/boao1$ $2 \cdot 2!(2^2 \cdot 3!)^2 168 \cdot 2$	2,534,400	14	64	319	960	1380
Q_{24}	$d_6^4(b)/aoao/boa^2/oaoa'/oba'a$ $(2^2 \cdot 3!)^4 \cdot 8$	739,200	12	64	327	960	1368
R_{24}	$d_6^2d_8 + 4/b^2o1^4/bob1^2 0^2/o^2a01^2 0/ao^2 01^3/oao1^3 0$ $(2^2 \cdot 3!)^2 2^3 \cdot 4! \cdot 2$	8,870,400	12	64	327	960	1368
S_{24}	$d_4d_6^3 + 2/abo^2 1^2/oaob10/aob^2 0^2/boao01/bo^2a10$ $2 \cdot 2!(2^2 \cdot 3!)^3 \cdot 2$	17,740,800	10	64	335	960	1356

4. **General enumeration theorems.** The following theorems, and others, were used to check Table I.

THEOREM 2. *Let* $\alpha_C(x) = \Sigma_{i=0}^{n} \alpha_i x^i$ *be the weight enumerator of* C. *Then*

$$\sum \alpha_C(x) = \prod_{j=1}^{n/2-2} (2^j + 1) \cdot \left[2^{n/2-1}(1 + x^n) + \sum_{2|i} \binom{n}{i} x^i \right],$$

where the sum extends over all self-dual codes C *of even length* n.

THEOREM 3. *If* n *is even, the number of self-dual codes with length* n *and minimum weight* $\geqslant 4$ *is*

$$\sum_{i=0}^{n/2} \frac{(-1)^i n!}{2^i i!(n-2i)!} \prod_{j=1}^{n/2-i-1} (2^j + 1).$$

TABLE I

Indecomposable Self Dual Codes of Length 24 (Page 3)

Code	Generator Matrix Order of Group	Number $\div \nu$	α_4	α_6	α_8	α_{10}	α_{12}
T_{24}	$d_4^4 d_8 / babab / ba^2oa / oab^2a' / aoba^2 / b^2oaa'$ $4^4 \cdot 2^3 \cdot 4! \cdot 8$	4,989,600	10	64	335	960	1356
U_{24}	$d_4^2 d_6^2 + 4 / ob^2o1^20^2 / oa^2o0^31 / obob0^21^2 / oaoa010^2 / b^2o^21^4 / a^2o^21010$ $4^2(2^2 \cdot 3!)^2 \cdot 4$	53,222,400	8	64	343	960	1344
V_{24}	$d_4^6(b) / babo^3 / obabo^2 / o^2babo / o^3bab / bo^3ba / abo^3b$ $4^6 \cdot 6 \cdot 8$	9,979,200	6	64	351	960	1332
W_{24}	$d_4^3 d_6 + 6 / \cdots$ $4^3 \cdot 2^2 \cdot 3! \cdot 3! \cdot 2$	106,444,800	6	64	351	960	1332
X_{24}	$d_4^4 + 8 / \cdots$ $4^4 \cdot 4! \cdot 2$	159,667,200	4	64	359	960	1320
Y_{24}	$d_4^2 + 16\text{-}o / \cdots$ $2^{11} \cdot 3^2$	106,444,800	2	64	367	960	1308
Z_{24}	see §3 $2^{10} \cdot 3^3 \cdot 5$	14,192,640	0	64	375	960	1296
Total:		$556{,}041{,}557 \frac{86}{1127} \cdot \nu$					

REFERENCES

1. E. F. Assmus, Jr. and H. F. Mattson, *Perfect codes and the Mathieu groups*, Arch. Math. (Basil) 17 (1966), 121–135. MR 34 #4050.

2. H.-V. Niemeier, *Definite quadratische Formen der Dimension* 24 *und Diskriminante* 1, J. Number Theory 5 (1973), 142–178.

3. Vera Pless, *On the uniqueness of the Golay codes,* J. Combinatorial Theory 5 (1968), 215–228.

4. ———, *A classification of self-orthogonal codes over GF*(2), Discrete Math. 3 (1972), 209–246. MR 46 #3200.

5. Vera Pless and N. J. A. Sloane, *On the classification and enumeration of self-dual codes* J. Combinatorial Theory.

6. J. A. Todd, *A representation of the Mathieu group* M_{24} *as a collineation group,* Ann. Mat. Pura Appl. (4) 71 (1966), 199–238. MR 34 #2713,

ELECTRICAL ENGINEERING DEPARTMENT, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MASSACHUSETTS 02139

BELL TELEPHONE LABORATORIES INC., MURRAY HILL, NEW JERSEY 07974