On Ternary Self-Dual Codes of Length 24

JEFFREY S. LEON, VERA PLESS, AND N. J. A. SLOANE, FELLOW, IEEE

Abstract—A partial classification is given of the self-dual codes of length 24 over GF(3). The main results are as follows: there are exactly two codes with minimum Hamming distance $d=9$; most of the codes have $d=6$ and are indecomposable; one code with $d=6$ has a trivial automorphism group (this is the first such self-dual code that has been found); the codes generated by the 59 inequivalent 24×24 Hadamard matrices have been investigated and there appear to be only nine inequivalent codes (two with $d=9$ and seven with $d=6$); and in all there are 27 decomposable codes, at least 96 indecomposable codes with $d=6$, and the total number of inequivalent codes is at least 140.

$$Q_{24}\quad \begin{array}{c|ccccccccccccccccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0
\end{array}$$

(a)

$$P_{24}\quad \begin{array}{cccccccccccc|c|ccccccccccc}
1 &&&&&&&&&&&& 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \cline{13-24}
& 1 &&&&&&&&&&& 2 & 0 & 1 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 \\
&& 1 &&&&&&&&&& 2 & 2 & 0 & 1 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 \\
&&& 1 &&&&&&&&& 2 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 1 & 2 & 2 & 2 \\
&&&& 1 &&&&&&&& 2 & 2 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 1 & 2 & 2 \\
&&&&& 1 &&&&&&& 2 & 2 & 2 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 1 & 2 \\
&&&&&& 1 &&&&&& 2 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 1 \\
&&&&&&& 1 &&&&& 2 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 2 & 1 & 1 \\
&&&&&&&& 1 &&&& 2 & 1 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 2 & 1 \\
&&&&&&&&& 1 &&& 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 2 \\
&&&&&&&&&& 1 && 2 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 \\
&&&&&&&&&&& 1 & 2 & 1 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 & 0
\end{array}$$

(b)

Fig. 1. Generator matrices for quadratic residue code Q_{24} and symmetry code P_{24}, the only two ternary self-dual codes of length 24 with minimum distance 9.

I. Summary of Results

The ternary self-dual codes with a length less than or equal to 20 have been completely classified in [4], [8], and [11]. This paper gives a partial classification of the ternary self-dual codes of length 24. The following are the main results.

1) There are exactly 27 decomposable codes (see Section II).

2) Let the numbers T_i be defined by

$$T_i=\sum_C \frac{1}{|\mathrm{Aut}(C)|}, \qquad i=0,1,\cdots,8,$$

where the sum is over all indecomposable inequivalent codes C containing exactly $2i$ codewords of weight 3. Let us say that a code is of *type* ie_3+je_4 if it contains exactly $2i+8j$ codewords of weight 3 and these codewords form a code equivalent to $ie_3 \oplus je_4$ (see [11]). Then T_i gives the total "mass" of the indecomposable codes of type ie_3. These numbers are derived in Section III and are shown in Table I.

3) A computer program has been developed to find the full automorphism group of a code. This program will be described in detail later [6].

4) There is a close connection between certain ternary self-dual codes of length 24 and the Hadamard matrices of order 24. The latter have recently been classified: there are exactly 59 inequivalent matrices [5]. Any of these matrices generates a self-dual code of length 24 (see Theorem 4). Using the computer program described in 3), we have investigated the codes generated by these 59 matrices and their transposes: there are exactly two codes with minimum distance $d=9$ (see 5) below), and it appears that there are seven inequivalent codes with $d=6$ (see Section IV).

5) Among all the self-dual codes of length 24 (not just those generated by Hadamard matrices) there are precisely two inequivalent codes with minimum distance 9 (see Theorem 6). These codes are the quadratic residue code Q_{24} and the symmetry code P_{24} ([7, chapter 16, §8], [10]). Both are indecomposable. Generator matrices for these two codes are given in Fig. 1. The automorphism groups are $\mathrm{Aut}(Q_{24}) = 2\cdot PSL_2(23)$ and $\mathrm{Aut}(P_{24})=Z_4\cdot PGL_2(11)$, of orders $22\cdot 23\cdot 24$ and 5280 respectively ([7, p. 493], [8, p. 662]).

6) Most self-dual codes of length 24 have minimum distance 6 and are indecomposable (see Theorem 7).

7) In view of 5) and 6) we now concentrate on the indecomposable codes C with $d=6$. The possible primes that divide $|\mathrm{Aut}(C)|$ are 2, 3, 5, 7, 11, and 13 (Theorem 8), and there are unique codes which are fixed by automorphisms of orders 7 and 13 (Theorem 9). Using the computer program given in the Appendix, we generated 300 random codes. Their groups were determined by the computer program described in 3); naturally, most of them are small. One code was found with an automorphism group of order 2, the smallest possible value. A generator matrix is shown in Fig. 2. This is the first known example of a self-dual code with a trivial automorphism group. Combinatorial structures with trivial or almost trivial automor-

Manuscript received April 7, 1980; revised June 18, 1980. This work was supported in part by the National Science Foundation under Grant MCS 78-01458.

J. S. Leon and V. Pless are with the Mathematics Department, University of Illinois at Chicago Circle, Box 4348, Chicago, IL 60680.

N. J. A. Sloane is with the Mathematics Department, Bell Laboratories, Murray Hill, NJ 07974.

0018-9448/81/0300-0176$00.75 ©1981 IEEE

1 1 1 1 1 1	0 0 0 0 0 0	0 0 0 0 0 0	0 0 0 0 0 0
0 0 0 0 0 0	1 1 1 1 1 1	0 0 0 0 0 0	0 0 0 0 0 0
0 0 0 0 0 0	0 0 0 0 0 0	1 1 1 1 1 1	0 0 0 0 0 0
2 1 0 0 0 0	1 1 1 0 0 0	0 0 0 0 0 0	0 0 0 0 1 0
0 2 1 0 0 0	0 0 0 0 0 0	1 1 1 0 0 0	0 0 0 0 1 0
0 0 2 1 0 0	0 0 0 1 2 0	1 0 0 2 0 0	0 0 0 0 0 0
0 0 0 2 1 0	0 0 0 1 0 2	0 0 0 0 0 0	1 2 0 0 0 0
0 0 0 0 2 1	0 0 0 0 0 0	0 0 0 0 1 2	1 0 2 0 0 0
1 0 0 0 0 2	0 0 0 0 0 0	0 2 0 0 1 0	0 0 0 0 1 1
0 0 0 0 0 0	1 2 0 0 0 0	0 0 0 0 0 0	1 1 1 1 0 0
2 0 0 0 1 0	0 2 0 0 0 1	0 0 0 0 0 0	0 0 2 0 0 1
0 0 0 0 0 0	0 0 0 1 2 0	1 0 2 0 0 0	0 1 0 2 0 0

Fig. 2. Generator matrix for the (probably unique) code with automorphism group of order 2. For this code $A_3 = 0$, $A_6 = 40$, and the hexad graph $\Gamma = 8C_0^1 + 4C_2^3$.

TABLE I
THE VALUES OF T_i

i	T_i
8	0
7	$1/80621568 \approx 1.24 \times 10^{-8}$
6	$23/89579520 \approx 2.57 \times 10^{-7}$
5	$23/6718464 \approx 3.42 \times 10^{-6}$
4	$5233/107495424 \approx 4.87 \times 10^{-5}$
3	$452689/560431872 \approx 8.08 \times 10^{-4}$
2	$567913/34836480 \approx 0.0163$
1	$19968947/51321600 \approx 0.389$
0	$61084634179343/6874630963200 \approx 8.8855147$

phism groups have recently been studied in other areas [1], [9].

8) Since the codes with $d = 9$ are the most interesting we curtailed our search at this point. The results are summarized in Table II. The total number of inequivalent codes is at least 140. (The precise number is probably much larger.) The codes shown with $d = 6$ contribute about 7.8886 to T_0, leaving $0.9969 \cdots$ to be accounted for. If the need arises we believe that the classification could be completed, although the analysis will become extremely tedious. Further progress could be facilitated if a computer program were available for determining whether two codes are equivalent, but no such program presently exists. Such a program could be used, for example, to show that the Hadamard matrices of order 24 give rise to *exactly* nine inequivalent codes.

9) The weight distribution of any of these codes is determined by the number of words of weights 3 and 6 (i.e. by A_3 and A_6), as shown in Table III.

The following sections give further information about these results.

II. DECOMPOSABLE CODES AND CODES WITH $d = 3$

The 27 decomposable codes are easily found from the shorter codes given in [11]. There is a unique decomposable code with minimum distance 6, namely the direct sum of two copies of the Golay code g_{12}. (This code is the Hadamard code H_1 in Section IV.) The rest have $d = 3$. The groups of these codes are quite large, the smallest group order being $2^{13} \cdot 3 = 24576$.

As for the indecomposable codes with minimum distance 3, one can show that there are respectively 0, 1, and 4 indecomposable codes of types $8e_3$, $7e_3$, and $6e_3$. We did not attempt to find the codes of types $5e_3, 4e_3, \cdots$.

TABLE II
SUMMARY OF TERNARY SELF-DUAL CODES OF LENGTH 24

Decomposable: 27 codes

Indecomposable

Minimum distance 3: At least 13 codes.

Type:	$8e_3$	$7e_3$	$6e_3$	$5e_3$	$4e_3$	$3e_3$	$2e_3$	e_3
Number:	0	1	4	≥2	≥2	≥2	≥2	≥2

Minimum distance 6: At least 96 codes.

Group	Number	Group	Number	Group	Number
2	≥1	128	≥1	276480	≥1
4	≥14	192	≥1	373248	≥2
8	≥14	256	≥1	622080	≥1
12	≥4	960	≥1	8294400	≥1
16	≥18	3072	≥1	88957440	1
24	≥5	3456	≥1	missing	≥4
32	≥8	8192	≥1		
48	≥5	31104	≥1		
64	≥5	49152	≥1		
96	≥2	241920	1		

Minimum distance 9: Exactly 2 codes.

TABLE III
THE WEIGHT DISTRIBUTION $\{A_i\}$ OF A SELF-DUAL CODE OF LENGTH 24 EXPRESSED IN TERMS OF A_3 AND A_6

A_0	=	1				
A_3	=			$1 \cdot A_3$		
A_6	=					$1 \cdot A_6$
A_9	=	4048	+	$249 \cdot A_3$	−	$6 \cdot A_6$
A_{12}	=	61824	−	$308 \cdot A_3$	+	$15 \cdot A_6$
A_{15}	=	242880	−	$564 \cdot A_3$	−	$20 \cdot A_6$
A_{18}	=	198352	+	$1029 \cdot A_3$	+	$15 \cdot A_6$
A_{21}	=	24288	−	$386 \cdot A_3$	−	$6 \cdot A_6$
A_{24}	=	48	−	$21 \cdot A_3$	+	$1 \cdot A_6$

III. THE T NUMBERS

The numbers T_i were defined in Section I. There are two quite different ways of computing them. The first requires that a complete list of the 27 decomposable codes of length 24 be available (as it is from Section II), and makes use of the following analog of Theorem 2 of [4].

Theorem 1: For $i = 8, 7, \cdots, 1, 0$ we have

$$\sum_{j=1}^{27} \frac{m_i(j)}{g(j)} + \sum_{s=i+1}^{8} \binom{s}{i} T_s + T_i = \frac{(1+1)(3+1)(3^2+1)\cdots(3^{11-i}+1)}{i!12^i \cdot 2^{24-3i}(24-3i)!},$$

where $m_i(j)$ is the number of times the code ie_3 occurs as a subcode of the jth decomposable code of length 24, and $g(j)$ is the order of the automorphism group of that code.

From this theorem, the values of $T_8, \cdots, T_0$ can be successively computed and are shown in Table I. The second method does not distinguish between decomposable and indecomposable codes but has the advantage of not requiring the initial list of decomposable codes. Thus it can be used in situations where the codes of shorter length have not yet been classified. Suppose we wish to classify the codes of length n. For all pairs of nonnegative integers i,j with $3i+4j \leq n$ we define

$$T'_{ij} = \sum_{C} \frac{1}{|\mathrm{Aut}(C)|},$$

where the sum is over all (decomposable *or* indecomposable) inequivalent ternary self-dual codes C of length n and type $ie_3 + je_4$.

Theorem 2: The numbers $T'_{i,j}$ may be obtained recursively from

$$T'_{i,j} = \frac{(1+1)(3+1)(3^2+1)\cdots(3^{n/2-i-2j-1}+1)}{12^i \cdot i! \cdot 48^j \cdot j!(n-3i-4j)!2^{n-3i-4j}} - \sum_{(k,l)\in S(i,j)} \sum_{m=i+j-l}^{\min\{i,k\}} 4^{i-m}\binom{k}{m}\binom{l}{j}\binom{l-j}{i-m} T'_{k,l}, \quad (1)$$

where $S(i,j)$ consists of all pairs of nonnegative integers k,l satisfying $(k,l) \neq (i,j)$, $i+j \leq k+l$, $3k+4l \leq n$, and $j \leq l$.

Proof: The first term on the right side of (1) is the total number of ternary self-dual codes of length n containing a subcode $ie_3 \oplus je_4$ (compare [4, theorem 1]). Suppose such a code has type $ke_3 + le_4$. Certainly the last three inequalities in the statement of the theorem must hold. Furthermore these codes can be divided into those with $(k,l)=(i,j)$, giving the term on the left side of (1), and those with $(k,l) \neq (i,j)$, corresponding to the last term in (1). Let us consider in how many ways a code of type $ke_3 + le_4$ can contain one of type $ie_3 + je_4$. We must first choose j out of the l copies of e_4, and then some number m of the k copies of e_3 and $(i-m)$ out of the remaining $(l-j)$ copies of e_4. Each of the last $(i-m)$ choices can be made in four ways. Thus (1) follows. Q.E.D.

Once the $T'_{i,j}$ have been calculated we can obtain the values of T_i from

$$T_i = T'_{i,0} - \sum_{C} \frac{1}{|\mathrm{Aut}(C)|},$$

where the sum is over all decomposable codes C of length n and type ie_3. For $n=24$ we successively compute $T'_{8,0}, T'_{7,0}, T'_{6,1}, T'_{6,0}, T'_{5,2}, \cdots, T'_{0,0}$. We find that $T'_{8,0} = 1/7739670528$; hence $T_8 = 0$, and so $T'_{7,0} = T_7 = 1/80621568$, and so on, in agreement with Table I. Theorems 1 and 2 can be easily generalized to give the sum of $|\mathrm{Aut}(C)|^{-1}$ over all codes C containing a subcode of any specified type; compare with [4, theorem 2].

IV. Codes Generated by Hadamard Matrices

Theorem 3: Let C be a ternary self-dual code of length 24 and $d=9$. Then C contains exactly 48 codewords of weight 24, and these vectors form the rows of a Hadamard matrix and its negative.

Proof: We see from Table III (with $A_3 = A_6 = 0$) that $A_{24} = 48$. Without loss of generality we may assume that C contains the all-ones vector. Then the complete weight enumerator of C is given in [8, fig. 6], and in particular C contains 46 vectors of shape $1^{12}(-1)^{12}$ and two vectors $\pm(1^{24})$. Suppose C contains the vectors

$$\begin{aligned} v &= 1\ 1\ \cdots\ 1 \quad 1\ 1\ \cdots\ 1 \quad -1\ -1\ \cdots\ -1 \quad -1\ \cdots\ -1 \\ w &= \underbrace{1\ 1\ \cdots\ 1}_{i} \quad \underbrace{-1\ -1\ \cdots\ -1}_{12-i} \quad \underbrace{1\ 1\ \cdots\ 1}_{12-i} \quad \underbrace{-1\ \cdots\ -1}_{i} \end{aligned}$$

with $i \neq 0, 12$. Then $v \cdot w = 4i - 24$. Since $v \cdot w = 0$ over GF(3), $i = 3$, 6, or 9. If $i=3$ or 9, $v \pm w$ has weight 6, contradicting the fact that $d=9$. Therefore $i=6$, and $v \cdot w = 0$ over the reals. Thus C contains a Hadamard matrix and its negative. Q.E.D.

The next theorem gives a partial converse.

Theorem 4: If a 24×24 Hadamard matrix is used as the generator matrix of a code C, then C is self-dual.

Proof: Clearly $C \subseteq C^{\perp}$. Let $d_1, \cdots, d_{24}$ be the elementary divisors of H. Then $|\det H| = d_1 \cdots d_{24} = 24^{12} = 2^{36}3^{12}$. Therefore there are at most twelve 3s among the d_i, and $\mathrm{rank}_3(H) = \dim C \geq 12$. Thus $C = C^{\perp}$. Q.E.D.

The same proof applies whenever n is a multiple of 12 but not of 36. The self-dual code obtained must have minimum distance at least 6 because a codeword of weight 3 would force three columns of the Hadamard matrix to be dependent, an impossible task. For $n=12$ of course this constructs the Golay code g_{12}, as has been known for a long time (cf. [2], [7, p. 647]). By combining Theorems 3 and 4 we obtain the following result.

Theorem 5: A self-dual code of length 24 with $d=9$ is generated by a Hadamard matrix.

The computer program described in Section I, result 3) was now used to study the codes generated by the 59 inequivalent Hadamard matrices of order 24 and their transposes (cf. [5]). There are exactly two codes with $d=9$, namely Q_{24} and P_{24}, and none with $d=3$. The next theorem then follows from Theorem 5.

Theorem 6: There are exactly two inequivalent self-dual codes of length 24 and minimum distance 9, namely Q_{24} and P_{24}.

The remaining Hadamard codes have $d=6$, and there are at least seven inequivalent codes. We conjecture that there are exactly seven, but in the absence of a program for testing code equivalence we cannot assert this conjecture as a theorem. But from the weight distribution, the group order, the orbits of the automorphism group on the hexads and on the 24 coordinates positions, and from other parameters, it appears that every Hadamard code with $d=6$ is equivalent to one of these seven.

The first of these seven codes is the decomposable code $H_1 = g_{12} \oplus g_{12}$, when g_{12} is the Golay code. Generator matrices for $H_2, \cdots, H_6$ are shown in Fig. 3. These matrices have been transformed by hand into a form in which the rows all have weight 6 and some or all of the structure of the code is apparent. Much more of the structure will become visible if the reader will generate all the codewords of weight 6. The following are the main properties of these seven codes.

$H_1 = g_{12} \oplus g_{12}$ has $A_3 = 0$, $A_6 = 528$, $g = |\mathrm{Aut}(H_1)| = 72260812800$, and its hexad graph Γ (see [11]) is $2C_{40}^{132}$.

H_2 has $A_3 = 0$, $A_6 = 96$, $g = 31104$, $\Gamma = 8C_4^6$, and contains two copies of the [9, 3, 6] component code g_9 (see [11]).

H_3 has $A_3 = 0$, $A_6 = 144$, $g = 49152$, and $\Gamma = 6C_8^{12}$.

H_4 has $A_3 = 0$, $A_6 = 48$, $g = 960$, and $\Gamma = 24C_0^1$.

H_5 has $A_3 = 0$, $A_6 = 240$, $g = 8294400$, and $\Gamma = 4C_{16}^{30}$. This code contains two copies of a new component code, γ_{12}, which is the [12, 5, 6] code generated by the first 5 rows of Fig. 3(d). γ_{12} is a subcode (or hyperplane) in g_{12}, and has weight distribution $A_0 = 1$, $A_6 = 90$, $A_9 = 140$, and $A_{12} = 12$. As glue vectors we may take $\pm x, \pm y, \pm x \pm y$ where $x = 000012\ 000000$ and $y = 000000\ 010221$. Furthermore $|\mathrm{Aut}(\gamma_{12})| = 2^6 \cdot 3^2 \cdot 5 = 2880$.

H_6 has $A_3 = 0$, $A_6 = 48$, $g = 3072$, and $\Gamma = 24C_0^1$.

H_7 has $A_3 = 0$, $A_6 = 96$, $g = 3456$, and $\Gamma = 8C_4^6$. We end this section with a corollary to Theorem 6.

Theorem 7: Most self-dual codes of length 24 are indecomposable and have $d=6$.

Proof: The number of distinct codes containing exactly $2i$ words of weight 3 is $2^{24} \cdot 24! \cdot T_i$. From Table I we see that T_0 is very much larger than the other T_i. Now T_0 is the sum of $|\mathrm{Aut}(C)|^{-1}$ over the codes with both $d=6$ and $d=9$, but from Theorem 6 the contribution from the codes with $d=9$ is negligible. The assertion of the theorem now follows. Q.E.D.

IV. The Possible Group Orders

Theorem 8: If C is a self-dual code of length 24 with $d=6$, then only the primes 2, 3, 5, 7, 11, and 13 can divide $|\mathrm{Aut}(C)|$.

Proof: We must eliminate 17, 19, and 23. Suppose C is fixed by an element σ of order 17. It follows from a theorem of Hering ([1], [3]) that the subcode of C consisting of vectors fixed by σ has dimension 4. The remaining $3^{12} - 3^4$ codewords of C are divided into sets of 17 under the action of σ, but $3^{12} - 3^4$ is not a multiple of 17, a contradiction. A similar argument eliminates 19. If 23 divides $|\mathrm{Aut}(C)|$, then C is an extended cyclic code and hence is equivalent to Q_{24}, which has $d=9$. Q.E.D.

Theorem 9: There is a unique code with $d=6$ that admits an automorphism of order 7, namely the code

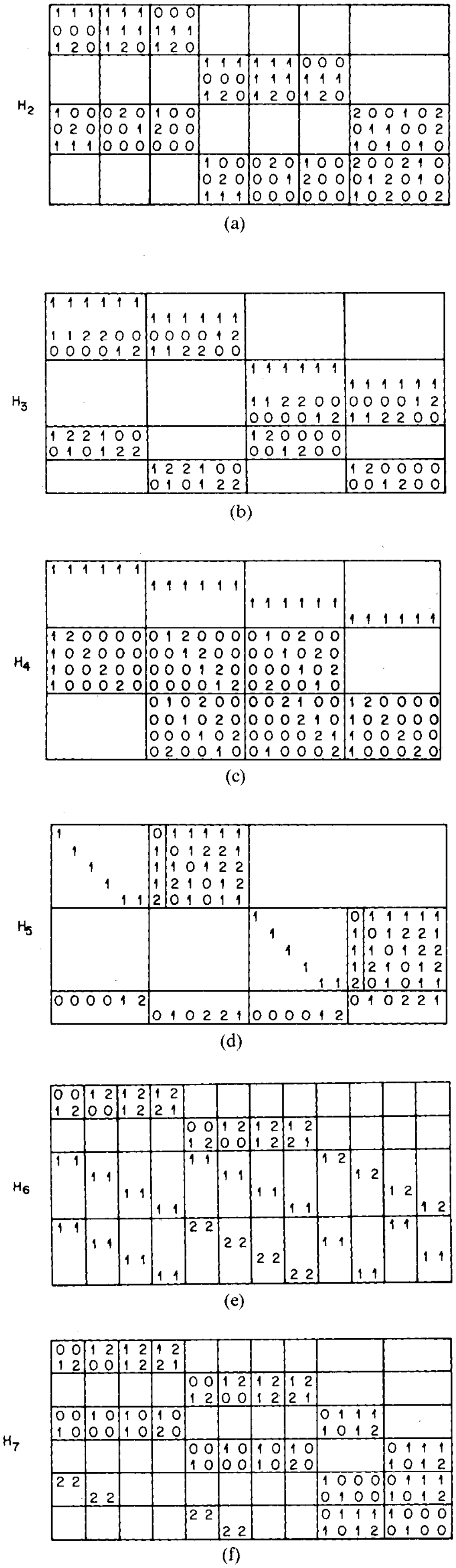

Fig. 3. Generator matrices for Hadamard codes $H_2, \cdots, H_7$.

g_{10}	0
0	η_{14}
x + y x − y	x y

Fig. 4. The code $g_{10}+\eta_{14}$, with group order $2^8\cdot 3^3\cdot 5\cdot 7=241920$.

g_{11}	0
0	p_{13}
u	t_0

Fig. 5. The code $g_{11}+p_{13}$, with group order $2^9\cdot 3^5\cdot 5\cdot 11\cdot 13=88957440$.

$g_{10}+\eta_{14}$ shown in Fig. 4. Similarly the code $g_{11}+p_{13}$ shown in Fig. 5 is the unique code admitting an element of order 13.

Proof: Suppose C has $d=6$ and admits an automorphism σ of order 7. From Section II we may assume that C is indecomposable. If σ has i cycles of length 7 and $24-7i$ fixed points, then by Hering's theorem the invariant subcode C' has dimension $(1/2)(24-6i)=12-3i$. As in the proof of Theorem 8 we must have $3^{12}\equiv 3^{12-3i}$ (mod 7), which implies $i=2$. Then (compare [3]) C' corresponds to a [12, 6, 6] self-dual code, which must be g_{12}. Therefore, on the ten fixed points of σ, C contains a component g_{10}. The complementary component of C on the remaining 14 coordinates is a [14, 6, 6] code with group order divisible by 7. From [11] we see that the only possibility is η_{14}. Finally there is a unique way to glue the components g_{10} and η_{14} together. The proof of the second assertion is similar. Q.E.D.

These two codes are included in Table II, as are the unique codes of types $g_{10}+p_{12}$ and $g_{10}+h_{14}$, and two codes of type $2p_{12}$. It is worth mentioning that the two $2p_{12}$ codes have different weight distributions but isomorphic groups.

Acknowledgment

The CAMAC computer system at the University of Illinois at Chicago Circle was used to find the automorphism group and other properties of these codes, and further processing of the codes was performed on the Honeywell computer at Bell Laboratories. V. Pless wishes to thank Dartmouth College for its hospitality while part of this work was carried out. We are very grateful to an anonymous referee for a number of helpful comments.

Appendix
Algorithm to Generate a Random Self-Orthogonal Code over GF(3)

Aim: Generate a random self-orthogonal $[n,k]$ code over GF(3) spanned by vectors $\boldsymbol{v}_r=(v_r(1),\cdots,v_r(n))$, for $r=1,\cdots,k$. Given vectors $\boldsymbol{v}_1,\cdots,\boldsymbol{v}_i$ spanning an $[n,i]$ code, the algorithm finds $\boldsymbol{v}_{i+1}$, $(i=0,1,\cdots,k-1)$. The coordinates $B_1,\cdots,B_i$ are such that $v_r(B_s)=\delta_{rs}$, and $B(i)$ denotes $\{1,2,\cdots,n\}-\{B_1,\cdots,B_i\}$.

Program:

```
i ← 0;
while i < k do
  begin
  for each j ∈ B(i) do u(j) ← RAND(GF(3));
  for l ← 1 until i do u(B_l) ← −Σ_{j∈B(i)} v_l(j)u(j);
  if u·u = 0 then
    begin
    u ← u − u(B_1)v_1 − ··· − u(B_i)v_i;
    if u ≠ 0 then
      begin
      i ← i + 1;
      Choose B_i with u(B_i) ≠ 0;
      u ← u(B_i)^{−1} u;
      for l ← 1 until i − 1 do
        v_l ← v_l − v_l(B_i)u;
      v_i ← u
      end
    end
end
```

References

[1] R. P. Anstee, M. Hall Jr., and J. G. Thompson, "Planes of order 10 do not have a collineation of order 5," preprint.

[2] E. F. Assmus, Jr., and H. F. Mattson, "Perfect codes and the Mathieu groups," *Archiv. der Mathematik*, vol. 17, pp. 121–135, 1966.

[3] J. H. Conway and V. Pless, "On primes dividing the order of a doubly-even (72, 36, 16) code and the group order of a quaternary (24, 12, 10) code," *Discrete Math.*, to be published.

[4] 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*, vol. IT-25 pp. 312–322, 1979.

[5] N. Ito, J. S. Leon, and J. Q. Longyear, "The 24-dimensional Hadamard matrices and their automorphism groups," *J. Combinatorial Theory*, (A), to be published.

[6] J. S. Leon, to be published.

[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North Holland and New York: Elsevier/North-Holland, 1977.

[8] C. L. Mallows, V. Pless, and N. J. A. Sloane, "Self-dual codes over GF(3)," *SIAM J. Appl. Math.* vol. 31, pp. 649–666, 1976.

[9] E. T. Parker and R. B. Killgrove, "A planar Latin square lacking automorphism," *J. Combinatorial Theory*, vol. 27A, pp. 404–406, 1979.

[10] V. Pless, "Symmetry codes over GF(3) and new five-designs," *J. Combinatorial Theory*, vol. 12, pp. 119–142, 1972.

[11] V. Pless, N. J. A. Sloane, and H. N. Ward, "Ternary codes of minimum weight 6, and the classification of the self-dual codes of length 20," *IEEE Trans. Inform. Theory*, vol. IT-26 pp. 305–316, May 1980.