New Extremal Ternary Self-Dual Codes

Masaaki Harada*

Department of Mathematics
Okayama University
Okayama 700, Japan

Dedicated to Professor Hiroshi Kimura on His 60th Birthday

Abstract

Compared to binary self-dual codes, few methods are known to construct ternary self-dual codes. In this paper, a construction method for ternary self-dual codes is presented. Using this method, a number of new extremal ternary self-dual codes are obtained from weighing matrices. In addition, a classification is given for extremal ternary self-dual codes of length 40 constructed from Hadamard matrices of order 20.

1 Introduction

A linear $[n, k]$ code C over $GF(p)$ is a k-dimensional vector subspace of $GF(p)^n$, where $GF(p)$ is the Galois field with p elements, p prime. The elements of C are called codewords and the weight $wt(x)$ of a codeword x is the number of its non-zero coordinates. The distance between codewords x and y is the weight $wt(x - y)$. The minimum weight of C is defined by $\min\{wt(x) \mid 0 \neq x \in C\}$. An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d. A matrix whose rows generate the code C is called a generator matrix of C. We say that the matrix generates C. Two codes C and C' over $GF(p)$ are *equivalent* if there exists an n by n monomial matrix P over $GF(p)$ with $C' = C \cdot P = \{xP \mid x \in C\}$. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in GF(p)^n \mid x \cdot y = 0 \text{ for all } y \in C\}$. C is *self-orthogonal* if $C \subseteq C^\perp$, and *self-dual* if $C = C^\perp$. Codes over $GF(3)$ are called *ternary*. A ternary self-dual $[n, n/2, d]$ code exists if and only if $n \equiv 0 \pmod 4$, and the minimum weight d is bounded by $d \leq 3[n/12] + 3$, where $[\ \ ]$ denotes the Gauss symbol (Mallows and Sloane [17]). If $d = 3[n/12] + 3$, the code is called *extremal*.

A weighing matrix $W(n, k)$ of order n and weight k is an n by n (0,1,−1)-matrix such that $W \cdot W^T = kI_n$, $k \leq n$, where I_n is the identity matrix of order n and W^T

*Current Address: Department of Mathematical Sciences, Yamagata University, Yamagata 990, Japan. This work was supported in part by a grant from the Japan Society for the Promotion of Science.

Australasian Journal of Combinatorics 17(1998), pp.133–145

denotes the transpose of W. A weighing matrix $W(n,n)$ is also called a Hadamard matrix. We say that two weighing matrices W_1 and W_2 of order n and weight k are *equivalent* if there exist monomial matrices of 0's, 1's and -1's P and Q such that $W_1 = P \cdot W_2 \cdot Q$.

All ternary self-dual codes of length ≤ 20 have been classified in [5], [16] and [21]. It was shown in [13] that there are exactly two inequivalent extremal self-dual $[24, 12, 9]$ codes. Two families of self-dual codes, namely the extended quadratic residue codes and the Pless symmetry codes, are well known (cf. [16]). In these families, the first few codes are extremal ternary self-dual codes. For larger lengths, extremal ternary self-dual codes exist for lengths ≤ 48, 56, 60 and 64, and do not exist for lengths 72, 96, 120, 144, ..., and the existence of extremal codes of other lengths is undecided (cf. [6, Section 7]). Recently Huffman [11] has enumerated extremal self-dual codes of lengths 28, 32 and 36 with monomial automorphisms of prime order $r \geq 5$ and length 40 with monomial automorphisms of prime order $r > 5$. It is the aim of this paper to construct a number of new extremal ternary self-dual codes from weighing matrices and Hadamard matrices. Table 1 contains information on the existence of known extremal ternary self-dual codes of length $n \leq 60$. In the table, the first, fourth and seventh columns denote the lengths n, the second, fifth and eighth columns give the number N of known inequivalent extremal codes of length n, and the third, sixth and ninth columns provide the references for these results.

Table 1: Known Extremal Ternary Self-Dual Codes

n	N	reference	n	N	reference	n	N	reference
4	1	[16]	24	2	[13]	44	≥ 1	[5]
8	1	[16]	28	≥ 14	[11]	48	≥ 2	[1], [20]
12	1	[16]	32	≥ 239	[11]	52	unknown	
16	1	[5]	36	≥ 1	[11], [20]	56	≥ 1	[5]
20	6	[21]	40	≥ 11	[2], [7], [11]	60	≥ 2	[1], [20]

Compared to binary self-dual codes, few methods are known to construct ternary self-dual codes. In Section 2, construction methods for ternary self-dual codes are presented. One of these methods is used in Section 4 to construct a number of new extremal ternary self-dual codes from weighing matrices. In Section 3, a classification is given for extremal ternary self-dual codes of length 40 constructed from Hadamard matrices of order 20.

Our notation and terminology follow from [4], [15] for coding theory, [8] for weighing matrices and [4], [12] for Hadamard matrices. We shall take the elements of $GF(3)$ to be either $\{0, 1, 2\}$ or $\{0, 1, -1\}$, using whichever form is more convenient.

2 Methods for Constructing Self-Dual Codes

In this section, several methods for constructing self-dual codes over $GF(p)$ (which includes ternary self-dual codes) are presented.

Proposition 2.1 *Let A be an n by n matrix over $GF(p)$ with $A \cdot A^T = kI_n$ over $GF(p)$ and let B be an n by n matrix over $GF(p)$ where p is prime and k is a positive integer $(0 < k < p)$. Let P be an n by n monomial matrix of 0's, 1's and -1's. If the matrix $[\ A\ ,\ B\ ]$ generates a self-dual code over $GF(p)$, then the following matrix*

$$G = [\ A\ ,\ P \cdot B\ ],$$

generates a self-dual $[2n, n]$ code over $GF(p)$.

Proof. The matrix $[\ A\ ,\ B\ ]$ generates a self-dual code over $GF(p)$ if and only if $B \cdot B^T = (p-k)I_n$ over $GF(p)$. If $B \cdot B^T = (p-k)I_n$ over $GF(p)$ then $(P \cdot B) \cdot (P \cdot B)^T = (p-k)I_n$ over $GF(p)$. Thus G generates a self-dual code over $GF(p)$. □

This method is trivial, but with this proposition and a generator matrix $[\ A\ ,\ B\ ]$ of a self-dual code with $A \neq I_n$, many different generator matrices can be obtained which may generate inequivalent self-dual codes. Thus this method is a useful tool for constructing new codes.

In Section 4, extremal ternary self-dual codes are constructed from weighing matrices using the following corollary, which is a special case of Proposition 2.1.

Corollary 2.2 *Let A be an n by n $(0, 1, -1)$-matrix with $A \cdot A^T = I_n$ over $GF(3)$ and let B be an n by n $(0, 1, -1)$-matrix with $B \cdot B^T = 2I_n$ over $GF(3)$. Let S_n be the symmetric group of degree n and let σ be an element of S_n where S_n acts on the set of all rows of the matrix B. Let $B^\sigma = [{b_{\sigma^{-1}(1)}}^T, \ldots, {b_{\sigma^{-1}(n)}}^T]^T$ be the matrix obtained from B by a permutation σ, where b_i is the i-th row of B. Then the following matrix*

$$G^\sigma = [\ A\ ,\ B^\sigma\ ],$$

generates a ternary self-dual code of length $2n$.

The matrices A and B in Corollary 2.2 are called type (I) and type (II) matrices, respectively, in Ozeki [19]. A method to construct ternary self-dual codes was given in [19] using these matrices. Note that the method given here is different from the one in [19].

Now a method for constructing ternary self-dual codes using Hadamard matrices is described. This method is well known (cf., e.g. [2], [5] and [7]).

Proposition 2.3 *Let H_n be a Hadamard matrix of order $n = 2$ or $n \equiv 8 \pmod{12}$. Then the following matrix*

$$G_{H_n} = [\ I_n\ ,\ H_n\ ],$$

generates a ternary self-dual code C_{H_n} of length $2n$.

Beenker [2] and Dawson [7] constructed extremal ternary self-dual codes of lengths 40 and 64 from certain Hadamard matrices using Proposition 2.3. In Section 3, a complete classification of extremal ternary self-dual $[40, 20, 12]$ codes constructed from all Hadamard matrices of order 20 is given. Hadamard matrices which generate extremal ternary self-dual $[64, 32, 18]$ codes are also discussed.

3 Extremal Self-Dual Codes from Hadamard Matrices

This section investigates extremal ternary self-dual codes constructed from Hadamard matrices. First the inequivalence of ternary self-dual codes derived from Hadamard matrices of order 20 is discussed. Although the following lemma is somewhat trivial, it is useful when classifying self-dual codes constructed from Hadamard matrices of fixed order.

Lemma 3.1 *Let H and H' be two equivalent Hadamard matrices of order n. Then the ternary self-dual codes constructed from H and H' by Proposition 2.3 are equivalent.*

Proof. Since H is equivalent to H', $H' = P \cdot H \cdot Q$, where P and Q are n by n monomial matrices of 0's, 1's and -1's. Thus it holds that

$$[\, I_n \,,\; H' \,] = [\, I_n \,,\; P \cdot H \cdot Q \,] = P\, [\, I_n \,,\; H \,]\, R,$$

where $R = \begin{bmatrix} P^{-1} & O \\ O & Q \end{bmatrix}$ is a $2n$ by $2n$ monomial matrix. Here O denotes the n by n zero matrix. Therefore the two codes are equivalent. □

Hall [10] proved that there are exactly three equivalence classes Q, P and N of Hadamard matrices of order 20. Denote the Hadamard matrices in classes Q, P and N by $H_{20,Q}, H_{20,P}$ and $H_{20,N}$ respectively. From Lemma 3.1, it is enough to consider only three inequivalent matrices in order to check the inequivalence of self-dual codes from all Hadamard matrices of order 20. Note that any Hadamard matrix of order 20 generates an extremal $[40, 20, 12]$ code by means of Proposition 2.3.

Now we present a method to distinguish between codes. Let C be a ternary self-dual $[2n, n, d]$ code. Let $M = (m_{ij})$ be an A_d by $2n$ matrix whose rows are codewords of weight d in C where A_i denotes the number of codewords of weight i in C. For an integer k $(1 \le k \le 2n)$, let $n(j_1, \ldots, j_k)$ be the number of r $(1 \le r \le A_d)$ such that $m_{rj_1} \cdots m_{rj_k} \neq 0$ for $1 \le j_1 < \cdots < j_k \le 2n$. We consider a set

$$S = \{n(j_1, \ldots, j_k) |\ \text{for any distinct } k \text{ columns } j_1, \ldots, j_k\ \}.$$

Let $M(k)$ and $m(k)$ be maximal and minimal numbers in S respectively. Since two equivalent codes have the same S, these numbers are invariant under the equivalence of codes. Since in this case the set of codewords of weight 12 forms a 3-design by the Assmus and Mattson theorem, we examine $M(4)$ and $m(4)$ in order to show the inequivalence of the codes constructed from the three inequivalent Hadamard matrices. These numbers are given in Table 2, and they result in the following theorem.

Table 2: Extremal Ternary [40, 20, 12] Codes from Hadamard Matrices

code	$M(4)$ (maximal number)	$m(4)$ (minimal number)
$C_{H_{20,Q}}$	144	72
$C_{H_{20,P}}$	216	88
$C_{H_{20,N}}$	312	72

Theorem 3.2 *Let H_{20} be a Hadamard matrix of order* 20. *Then the matrix* $[\ I_{20}\ ,\ H_{20}\ ]$ *generates an extremal ternary self-dual* [40, 20, 12] *code. Moreover there are exactly three inequivalent self-dual codes derived from all Hadamard matrices of order* 20.

Next, consider the extremal ternary self-dual [64, 32, 18] codes constructed from Hadamard matrices of order 32. Let P_{32} be the Paley type Hadamard matrix of order 32 (see [4] for the definition). We remark that the Hadamard matrices constructed by Construction 2 in [7] are Paley type Hadamard matrices. The first extremal [64, 32, 18] code was found by Beenker [2], and later Dawson [7] found an extremal code from P_{32} using Proposition 2.3. It was announced in [14] that there are at least 66104 inequivalent Hadamard matrices of order 32. It follows from [14] that all known matrices except P_{32} and ${P_{32}}^T$ are equivalent to $H_2 \otimes H_{16}$ or are of Kronecker type $K = \begin{bmatrix} K_1 & K_1 \\ K_2 & -K_2 \end{bmatrix}$ where K_1 and K_2 are Hadamard matrices of order 16, or the transpose of K. It is known [9] that there are exactly five inequivalent Hadamard matrices of order 16. Any Hadamard matrix of order 16 has a submatrix consisting of four rows which is equivalent to the following matrix

$$\begin{bmatrix} ++++ & ++++ & ++++ & ++++ \\ ++++ & ++++ & ---- & ---- \\ ++++ & ---- & ++++ & ---- \\ ++++ & ---- & ---- & ++++ \end{bmatrix}. \tag{1}$$

Throughout this paper, we denote 1 and -1 by $+$ and $-$ respectively. Thus the codes constructed from the matrices in [14] (except P_{32} and ${P_{32}}^T$) contain codewords of weight 12. Therefore in order to construct a new extremal code from a Hadamard matrix of order 32, one must construct a Hadamard matrix which is inequivalent to P_{32}, $H_2 \otimes H_{16}$, $H_4 \otimes H_8$ or Kronecker type K or their transposes. To date the existence of such a matrix is unknown.

Now consider the codes constructed in [2] and [7]. The code C_p in [2] has a generator matrix of the form $[\ I_{p+1}\ ,\ S\ ]$ where S is a Hadamard matrix when p is a prime of the form $p = 12k - 5$ (cf. [2]). As mentioned in [18], the two extremal $[64, 32, 18]$ codes in [2] and [7] are equivalent. In general the transpose S^T of S is equivalent to a Paley type Hadamard matrix, essentially since -1 is not a quadratic residue in this case. It follows from self-duality that the code C_p in [2] is equivalent to the code constructed from a Paley type Hadamard matrix when p is a prime of the form $p = 12k - 5$. Thus the codes $C_{H_{20,Q}}$ and C_{19} in [2] are equivalent.

Dawson [7] gave the following question: does a Paley Hadamard matrix of order n always generate a ternary self-dual code with minimum weight $n/2 + 2$ the construction in Proposition 2.3 is used? Beenker [2] found that the minimum weight of C_{43} in [2] is 18 or 21. Moreover C_{43} and the code constructed from the Paley Hadamard matrix of order 44 are equivalent. Thus we have the following:

Proposition 3.3 *Using Proposition 2.3, Paley Hadamard matrices of order n do not always generate ternary self-dual codes with minimum weight $n/2 + 2$.*

4 New Extremal Self-Dual Codes

In this section, a number of new extremal ternary self-dual codes are constructed from weighing matrices using Corollary 2.2. We also compare these new codes with known extremal codes.

First we present the construction of some weighing matrices. Let C and D be circulant matrices and R be the back diagonal matrix (see [8] for the definition of the back diagonal matrix). A weighing matrix is said to be *constructed from two circulant matrices* C and D if it is of the form

$$\begin{bmatrix} C & D \cdot R \\ D \cdot R & -C \end{bmatrix}.$$

Many weighing matrices of this type are given in [8].

Proposition 4.1 (Geramita and Seberry [8]) *There exist weighing matrices of order $2n$ and weight k constructed from two circulant matrices for*

(1) $n \geq 7,\ k \in \{0, 1, 2, 4, 5, 8, 10\}$;

(2) $n \geq 9,\ k \in \{0, 1, 2, 4, 5, 8, 10, 16\}$;

(3) $n \geq 11,\ k \in \{0, 1, 2, 4, 5, 8, 10, 13, 16, 20\}$.

4.1 Extremal [28,14,9] Codes

Let $W_{14,4}$, $W_{14,5}$ and $W_{14,10}$ be the weighing matrices constructed from two circulant matrices with the following first rows:

$$\begin{aligned} &++00000, \quad +-00000, \\ &+0+0000, \quad ++-0000 \text{ and} \\ &+0+--+0, \quad +0+++-0, \end{aligned}$$

respectively.

Using Corollary 2.2, 16 extremal ternary self-dual codes of length 28 have been constructed from $W_{14,4}$, $W_{14,5}$ and $W_{14,10}$. Table 3 lists for each code the chosen matrices, A and B, and the permutation σ in Corollary 2.2.

Table 3: Extremal Ternary [28, 14, 9] Codes from Weighing Matrices

code	A	B	σ
$C_{28,1}$	$W_{14,4}$	$W_{14,5}$	$(1,11,6)(2,10,5,14,9,4,13,8,3,12,7)$
$C_{28,2}$	$W_{14,4}$	$W_{14,5}$	$(1,2,10,4,12,6,14,8,9,3,11,5,13,7)$
$C_{28,3}$	$W_{14,4}$	$W_{14,5}$	$(1,3,11,5,13,7)(2,10,4,12,6,14,8)(9)$
$C_{28,4}$	$W_{14,4}$	$W_{14,5}$	$(1,14,13,12,3,2)(4,11,10,9,8,7,6,5)$
$C_{28,5}$	$W_{14,4}$	$W_{14,5}$	$(1,9,8,14,5,11,2,7,13,4,10)(3,6,12)$
$C_{28,6}$	$W_{14,4}$	$W_{14,5}$	$(1,3,2)(4,8,7,6,5)(9)(10)\dots(14)$
$C_{28,7}$	$W_{14,4}$	$W_{14,5}$	$(1,14,4,9,5,10,8,13,3,7,12,2,6,11)$
$C_{28,8}$	$W_{14,10}$	$W_{14,5}$	$(1,7,13,5,11,3)(2,8,14,6,12,4,10)(9)$
$C_{28,9}$	$W_{14,10}$	$W_{14,5}$	$(1,12,9,6,3,14,11,8,2,13,10,7,4)(5)$
$C_{28,10}$	$W_{14,10}$	$W_{14,5}$	$(1,11,7,3,13,4,14,10,6,2,12,8,9,5)$
$C_{28,11}$	$W_{14,10}$	$W_{14,5}$	$(1,7,14,9)(2,6,13,5,12,4,11,3,10)(8)$
$C_{28,12}$	$W_{14,10}$	$W_{14,5}$	$(1,8,7,6,5,4,3,2,14)(9)(10)(11)(12)(13)$
$C_{28,13}$	$W_{14,10}$	$W_{14,5}$	$(1,7,14,6,13,10,2,9)(3,5,12,4,11)(8)$
$C_{28,14}$	$W_{14,10}$	$W_{14,5}$	$(1,14,13,12,4,2,8,6,11,10,9,7,5,3)$
$C_{28,15}$	$W_{14,10}$	$W_{14,5}$	$(1,11,6)(2,12,7,10,5,8,3,13,9,4,14)$
$C_{28,16}$	$W_{14,10}$	$W_{14,5}$	$(1,9,10,11,12,13,2)(3,14,8,7,6,5,4)$

Now we compare the known extremal codes with the codes given here. Huffman [11] constructed 14 and 5 inequivalent ternary [28, 14, 9] codes with monomial automorphisms of order $r = 7$ and 13, respectively. Denote the 14 codes with an automorphism of order 7 by $C'_{28,1}, \dots, C'_{28,14}$, and the 5 codes with an automorphism of order 13 by $C''_{28,1}, \dots, C''_{28,5}$, according to the order in [11]. Here we use another equivalent invariant to show the inequivalence of some codes. Let d_i be the number of pairs of codewords with distance i among all minimum weight codewords. These numbers are invariant under the equivalence of ternary codes. Note that this method is essentially the same as the method for binary codes given in Tonchev [22]. For these codes, the values $M(4)$, $m(4)$, $M(5)$, $m(5)$ and d_i $(i = 9,\ 12,\ 15,\ 18)$ are listed in Table 4. It follows from this table that at least 16 codes are inequivalent.

Similarly, Table 5 lists the values $M(4)$, $m(4)$, $M(5)$, $m(5)$ and d_i $(i = 9, 12, 15, 18)$ for our codes constructed from weighing matrices. Table 5 implies that these 16 codes are new extremal codes. Tables 4 and 5 result in the following proposition.

Proposition 4.2 *There are at least* 32 *inequivalent extremal ternary self-dual codes of length* 28.

Table 4: Huffman's Extremal Ternary $[28, 14, 9]$ Codes

code	$M(4)$	$m(4)$	$M(5)$	$m(5)$	d_9	d_{12}	d_{15}	d_{18}
$C'_{28,1}$	24	2	10	0	105252	945504	1236312	96768
$C'_{28,2}$	24	0	6	0	99372	963144	1218672	102648
$C'_{28,3}$	24	4	10	0	103740	950040	1231776	98280
$C'_{28,4}$	24	0	10	0	103236	951552	1230264	98784
$C'_{28,5}$	24	0	10	0	103740	950040	1231776	98280
$C'_{28,6}$	24	0	10	0	103740	950040	1231776	98280
$C'_{28,7}$	24	0	12	0	103236	951552	1230264	98784
$C'_{28,8}$	24	0	10	0	103236	951552	1230264	98784
$C'_{28,9}$	20	0	8	0	108444	935928	1245888	93576
$C'_{28,10}$	24	0	10	0	103236	951552	1230264	98784
$C'_{28,11}$	24	0	10	0	103236	951552	1230264	98784
$C'_{28,12}$	20	0	10	0	104412	948024	1233792	97608
$C'_{28,13}$	24	0	10	0	104412	948024	1233792	97608
$C'_{28,14}$	16	0	6	0	99372	963144	1218672	102648
$C''_{28,1}$	24	0	6	0	99372	963144	1218672	102648
$C''_{28,2}$	24	0	6	0	99372	963144	1218672	102648
$C''_{28,3}$	16	0	6	0	99372	963144	1218672	102648
$C''_{28,4}$	24	0	10	0	103740	950040	1231776	98280
$C''_{28,5}$	24	0	8	0	103740	950040	1231776	98280

Table 5: Extremal Ternary $[28, 14, 9]$ Codes from Weighing Matrices

code	$M(4)$	$m(4)$	$M(5)$	$m(5)$	d_9	d_{12}	d_{15}	d_{18}
$C_{28,1}$	24	0	12	0	104340	948240	1233576	97680
$C_{28,2}$	24	0	10	0	104124	948888	1232928	97896
$C_{28,3}$	24	0	10	0	104172	948744	1233072	97848
$C_{28,4}$	24	0	10	0	104052	949104	1232712	97968
$C_{28,5}$	24	0	12	0	103836	949752	1232064	98184
$C_{28,6}$	24	0	12	0	103524	950688	1231128	98496
$C_{28,7}$	24	0	12	0	104100	948960	1232856	97920
$C_{28,8}$	24	0	10	0	104388	948096	1233720	97632
$C_{28,9}$	24	0	12	0	103956	949392	1232424	98064
$C_{28,10}$	24	0	12	0	104244	948528	1233288	97776
$C_{28,11}$	24	0	12	0	104676	947232	1234584	97344
$C_{28,12}$	24	0	10	0	103812	949824	1231992	98208
$C_{28,13}$	24	0	10	0	103908	949536	1232280	98112
$C_{28,14}$	24	0	12	0	103764	949968	1231848	98256
$C_{28,15}$	24	0	12	0	103668	950256	1231560	98352
$C_{28,16}$	24	0	12	0	103620	950400	1231416	98400

4.2 Extremal [40,20,12] Codes

At least three extremal ternary $[40, 20, 12]$ codes have been found using Corollary 2.2. The matrices and the permutations for these codes, as described in Corollary 2.2, are listed in Table 6. Here $W_{20,5}$, $W_{20,8}$, $W_{20,10}$ and $W_{20,16}$ are the weighing matrices constructed from two circulant matrices whose first rows are

$$\begin{array}{ll} & +0+0000000, \quad ++-0000000, \\ & +++-000000, \quad ++-+000000, \\ & +0+--+0000, \quad +0+++-0000 \\ \text{and} & +++-++-+00, \quad +++---+-00, \end{array}$$

respectively. The maximal and minimal numbers, $M(4)$ and $m(4)$, for the three codes are listed in Table 7.

Table 6: Extremal Ternary $[40, 20, 12]$ Codes from Weighing Matrices

code	A	B	σ
$C_{40,w1}$	$W_{20,10}$	$W_{20,5}$	$(1,10,9,\ldots,3,2)(11)(12)\cdots(20)$
$C_{40,w2}$	$W_{20,10}$	$W_{20,5}$	$(1,\ldots,10)(11,16)(12,17)(13,18)(14,19)(15,20)$
$C_{40,w3}$	$W_{20,16}$	$W_{20,8}$	$(1,12)(2,13)(3,14)(4,15)(5,16)(6,17)(7,18)(8,19)(9,20)(10,11)$

Table 7: Extremal Ternary $[40, 20, 12]$ Codes from Weighing Matrices

code	$M(4)$ (maximal number)	$m(4)$ (minimal number)
$C_{40,w1}$	160	48
$C_{40,w2}$	160	74
$C_{40,w3}$	176	72

Now we consider the inequivalence of these codes and the known extremal codes. Huffman [11] showed that there are exactly four and eleven inequivalent ternary $[40, 20, 12]$ codes with monomial automorphisms of order $r = 13$ and 19, respectively. As mentioned in [11], the equivalence or inequivalence of two extremal codes constructed from two different automorphism orders is still open. Thus the equivalence or inequivalence of the six codes in Section 3 and this section, and the above 15 codes, must be checked.

First, denote the four codes with an automorphism of order 13 by $C_{40,1}$, $C_{40,2}$, $C_{40,3}$ and $C_{40,4}$, and the 11 codes with an automorphism of order 19 by $C_{40,5}, \ldots, C_{40,15}$, according to the order in [11]. The maximal and minimal numbers $M(4)$ and $m(4)$ for these codes are listed in Table 8.

It follows from Table 8 and Theorem 2 in [11] that all codes except $C_{40,3}$ and $C_{40,13}$ are inequivalent. Since our computer search shows that the values d_{12} for the

Table 8: Huffman's Extremal Ternary [40, 20, 12] Codes

code	$M(4)$ (maximal)	$m(4)$ (minimal)	code	$M(4)$ (maximal)	$m(4)$ (minimal)
$C_{40,1}$	152	74	$C_{40,9}$	144	72
$C_{40,2}$	142	74	$C_{40,10}$	156	76
$C_{40,3}$	148	72	$C_{40,11}$	144	72
$C_{40,4}$	148	76	$C_{40,12}$	148	68
$C_{40,5}$	140	72	$C_{40,13}$	148	72
$C_{40,6}$	168	76	$C_{40,14}$	144	72
$C_{40,7}$	144	78	$C_{40,15}$	144	72
$C_{40,8}$	150	76			

two codes $C_{40,3}$ and $C_{40,13}$ are 2216968 and 2225584, these codes are inequivalent. Therefore we have the following proposition.

Proposition 4.3 *The* 15 *extremal ternary self-dual* [40, 20, 12] *codes with monomial automorphisms of order* $r > 5$ *in* [11] *are inequivalent.*

Now these 15 extremal codes are compared with the six codes constructed from weighing matrices and Hadamard matrices of order 20. The Hadamard matrix $H_{20,Q}$ has an automorphism of order 19 (cf. [10]). Since an element of order 19 induces an automorphism of order 19 in $C_{H_{20,Q}}$, it must have an automorphism of order 19. Hence this code must be equivalent to one of the 11 codes in [11].

Tables 2, 7 and 8 give the following proposition.

Proposition 4.4 *There are at least* 20 *inequivalent extremal ternary self-dual* [40, 20, 12] *codes.*

4.3 Extremal [44,22,12] Codes

By Proposition 4.1, we can construct weighing matrices of order 22 and weights 4, 16 and 20. The first rows of these matrices are the following:

$$
\begin{array}{ll}
++000000000, & +-000000000, \\
+++-++-+000, & +++---+-000 \text{ and} \\
+--+-+---+0, & +-------++-0,
\end{array}
$$

respectively. We denote these weighing matrices by $W_{22,k}$ with $k = 4$, 16 and 20. Similarly a weighing matrix denoted $W_{22,17}$ can be constructed using the following first row:

$$-+0+++000+0, \quad ++-+++---+-.$$

Using Corollary 2.2, six extremal ternary [44, 22, 12] codes have been constructed from weighing matrices $W_{22,4}$, $W_{22,16}$ and $W_{22,20}$. Table 9 lists for these codes the chosen matrices, A and B, and the permutation σ, in Corollary 2.2. Note that

Table 9: Extremal Ternary [44, 22, 12] Codes from Weighing Matrices

code	A	B	σ
$C_{44,1}$	$W_{22,4}$	$W_{22,20}$	$(1,22)(2,3,\ldots,20,21)$
$C_{44,2}$	$W_{22,4}$	$W_{22,20}$	$(1,11,21,9,19,7,17,5,15,3,13)(2,12,22,10,20,8,18,6,16,4,14)$
$C_{44,3}$	$W_{22,4}$	$W_{22,20}$	$(1,14,5,18,9,22,2,15,6,19,10)(3,16,7,20,11,13,4,17,8,21,12)$
$C_{44,4}$	$W_{22,4}$	$W_{22,20}$	$(1,22,21,\ldots,4,3,2)$
$C_{44,5}$	$W_{22,16}$	$W_{22,20}$	$(1,13,3,15,5,17,7,19,9,21,11,12,2,14,4,16,6,18,8,20,10,22)$
$C_{44,6}$	$W_{22,16}$	$W_{22,20}$	$(1,11,10,\ldots,4,3,2)(12,22,21,\ldots,15,14,13)$

$[\ I_{22}\ , W_{22,17}\ ]$ and $[\ I_{22}\ , W_{22,20}\ ]$ also generate extremal ternary self-dual codes of length 44. These codes are denoted by $C_{44,7}$ and $C_{44,8}$, respectively.

For length 44, $M(3)$ and $m(3)$ were determined for each of the eight codes, and these numbers are listed in Table 10. It follows from Table 10 that there are at least eight inequivalent extremal [44, 22, 12] codes which can be constructed from weighing matrices of order 22. In addition, Conway, Pless and Sloane [5] have constructed an extremal [44, 22, 12] code from the Pless symmetry [48, 24, 15] code by subtracting the unique [4, 2, 3] code.

Table 10: The Inequivalence of [44, 22, 12] Codes

code	$M(3)$ (maximal number)	$m(3)$ (minimal number)
$C_{44,1}$	176	100
$C_{44,2}$	168	84
$C_{44,3}$	178	104
$C_{44,4}$	174	96
$C_{44,5}$	170	100
$C_{44,6}$	170	84
$C_{44,7}$	184	88
$C_{44,8}$	174	84

4.4 Extremal Codes for Other Lengths

Many inequivalent ternary [32, 16, 9] codes were constructed in [11]. Thus only one example is given here of an extremal ternary code of length 32 constructed from a weighing matrix using Corollary 2.2. Let $W_{16,4}$ and $W_{16,5}$ be the weighing matrices constructed from two circulant matrices with the following first rows:

$$++000000, \quad +-000000 \text{ and}$$
$$+0+00000, \quad ++-00000,$$

respectively. Let C_{32} be a self-dual code with generator matrix of the form $[\ W_{16,4}\ ,\ W_{16,5}{}^{\sigma}\ ]$ where $\sigma = (1,7,12)(2,6,11,16,5,10,15,4,9,14,3,8,13)$. C_{32} is an extremal ternary self-dual code of length 32.

Let $W_{18,17}$ be the weighing matrix of order 18 and weight 17 constructed in [8] from two circulant matrices with first rows:

$$+--++++--, \quad 0-+-----+-.$$

It can easily be checked that the matrix [I_{18} , $W_{18,17}$] generates an extremal ternary self-dual code C_{36}. Only one extremal ternary self-dual code of length 36 is known. This is the Pless symmetry code P_{36} of length 36 (cf. [20]). Let [I_{q+1} , S_q] be the generator matrix of the Pless symmetry code of length $2(q+1)$. Since it follows from Theorem 2.1 in [20] that $S_q \cdot S_q{}^T = qI_{q+1}$, S_q is a weighing matrix of order $q+1$ and weight q. It is known [3] that there is a unique weighing matrix of order 18 and weight 17 up to equivalence. This implies that the two codes P_{36} and C_{36} are equivalent.

Similarly, the matrix [I_{30} , $W_{30,29}$] generates an extremal ternary self-dual code. $W_{30,29}$ as given in [8] can be constructed from two circulant matrices with first rows

$$0++--+-----+--++ \text{ and } +-+-----++-----+-.$$

Two inequivalent extremal [60, 30, 18] codes are known. These are the Pless symmetry code and the extended quadratic residue code (cf. [16]). The possible equivalence of these codes with the code given here has not been checked.

Acknowledgements. The author would like to thank his adviser Professor Hitoshi Kaneta for his helpful discussions and encouragement, Professor Hiroshi Kimura for reading a preliminary version of this paper, and Professor Michio Ozeki for his helpful advice on ternary self-dual codes. The author would also like to thank Professor T. Aaron Gulliver for his useful comments and suggestions on a preliminary version of this paper.

References

[1] E.F. Assmus, Jr., and H.F. Mattson, Jr., New 5-designs, *J. Combin. Theory* **6** (1969) 122–151.

[2] G.F.M. Beenker, A note on extended quadratic residue codes over $GF(9)$ and their ternary images, *IEEE Trans. Inform. Theory* **30** (1984) 403–405.

[3] H.C. Chan, C.A. Rodger and J. Seberry, On inequivalent weighing matrices, *Ars Combin.* **21** (1986) 299–333.

[4] P.J. Cameron and J.H. van Lint, Designs, Graphs, Codes and Their Links (Cambridge University Press, Cambridge, 1991).

[5] 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* **25** (1979) 312–322.

[6] J.H. Conway and N.J.A. Sloane, Sphere Packing, Lattices and Groups (Springer-Verlag, New York, 1988).

[7] E. Dawson, Self-dual ternary codes and Hadamard matrices, *Ars Combin.* **19** (1985) 303–308.

[8] A.V. Geramita and J. Seberry, Orthogonal Designs: Quadratic Forms and Hadamard Matrices (Marcel Dekker, New York, 1979).

[9] M. Hall, Jr., Hadamard matrices of order 16, J.P.L. Research Summary 36–10 1 (1961) 21–26.

[10] M. Hall, Jr., Hadamard matrices of order 20, J.P.L. Technical Report No. 32–761 (1965).

[11] W.C. Huffman, On extremal self-dual ternary codes of lengths 28 to 40, *IEEE Trans. Inform. Theory* **38** (1992) 1395–1400.

[12] E.S. Lander, Symmetric Designs: An Algebraic Approach (Cambridge University Press, Cambridge, 1983).

[13] J.S. Leon, V. Pless and N.J.A. Sloane, On ternary self-dual codes of length 24, *IEEE Trans. Inform. Theory* **27** (1981) 176–180.

[14] C. Lin, W.D. Wallis and Z. Lie, Equivalence classes of Hadamard matrices of order 32, *Congr. Numer.* **95** (1993) 179–182.

[15] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977).

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

[17] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. Control* **22** (1973) 188–200.

[18] M. Ozeki, Ternary code construction of even unimodular lattices, in: J.-M. De Koninck and C. Levesque, ed., Théoric de Nombres (Walter de Gruyter & Co., Berlin-New York, 1989) 772–784.

[19] M. Ozeki, On a class of self-dual ternary codes, *Sci. Rep. Hirosaki Univ.* **36** (1989) 184–191.

[20] V. Pless, Symmetry codes over $GF(3)$ and new five-designs *J. Combin. Theory Ser. A* **12** (1972) 119–142.

[21] V. Pless, N.JA. Sloane and H.N. Ward, Ternary codes of minimum weight 6 and the classification of self-dual codes of length 20, *IEEE Trans. Inform. Theory* **26** (1980) 305–316.

[22] V.D. Tonchev, Block designs of Hadamard type and self-dual codes, *Probl. Pered. Inform.* **19** (1983) 25–30 (in Russian). English translation in: *Probl. Inform. Trans.* **19** (1984) 270–275.

(Received 16/1/97)