Designs, Codes and Cryptography, 23, 11–21, 2001

Binary Optimal Odd Formally Self-Dual Codes

KOICHI BETSUMIYA Koichi@math.nagoya-u.ac.jp
Graduate School of Mathematics, Nagoya University, Nagoya 464-8602, Japan

MASAAKI HARADA harada@kszaoh3.kj.yamagata-u.ac.jp
Department of Mathematical Sciences, Yamagata University, Yamagata 990-8560, Japan

Communicated by: V. D. Tonchev

Received November 3, 1998; Revised September 28, 1999; Accepted November 15, 1999

Abstract. In this paper, we study binary optimal odd formally self-dual codes. All optimal odd formally self-dual codes are classified for length up to 16. The highest minimum weight of any odd formally self-dual codes of length up to 24 is determined. We also show that there is a unique linear code for parameters [16, 8, 5] and [22, 11, 7], up to equivalence.

Keywords: Odd formally self-dual codes, [22, 11, 7] code

1. Introduction

A binary linear $[n, k]$ code C is a k-dimensional vector subspace of $\mathbb{F}_2^n$, where $\mathbb{F}_2$ is the finite field of two elements. The elements of C are called codewords. The weight $wt(x)$ of a codeword x is the number of non-zero coordinates. The minimum weight of C is the smallest weight among all non-zero codewords of C. An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d. Two codes C and C' are equivalent if one can be obtained from the other by permuting the coordinates. The automorphism group of C is the set of permutations of the coordinates which preserve C. The weight enumerator of C is $W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$, where A_i is the number of codewords of weight i in C. When recording a weight enumerator, we shall set $x = 1$. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{F}_2^n \mid x \cdot y = 0 \text{ for all } y \in C\}$ where $x \cdot y$ denotes the standard inner-product of x and y.

A code C is *self-dual* if $C = C^\perp$. A code C is *formally self-dual* if C and $C^\perp$ have identical weight enumerators. Self-dual codes are by definition formally self-dual automatically. There exist formally self-dual codes which are not self-dual. In the remainder of this paper, the term formally self-dual code pertains to a non-self-dual code. A code is called *even* if the weights of all codewords are even. A formally self-dual code which is not even is called *odd*. In this paper, we deal with odd formally self-dual codes. The minimum weight of an even formally self-dual code of length n is bounded by $2\lfloor \frac{n}{8} \rfloor + 2$. An even formally self-dual $[n, n/2, 2\lfloor \frac{n}{8} \rfloor + 2]$ code is called extremal. The restrictions on odd formally self-dual codes are significantly fewer than on even formally self-dual codes. Thus there can be odd formally self-dual codes with minimum weight exceeding the above bound. This is one reason of interest in odd formally self-dual codes. An odd formally self-dual code with the highest minimum weight for that length is called *optimal*. An *optimal* formally self-dual code has the highest minimum weight among even formally self-dual codes as well as odd formally self-dual codes.

In Section 2, we give the classification of optimal odd formally self-dual codes of length up to 14. Section 2 also contains the current information on the highest minimum weight of odd formally self-dual codes of length up to 24. In Section 3, we show that there is a unique odd formally self-dual [22, 11, 7] code, up to equivalence. The codewords of the minimum weight in the unique odd formally self-dual [22, 11, 7] code form a unique quasi-symmetric 2-(22, 7, 16) design with intersection numbers 1 and 3. It is also shown that any linear [22, 11, 7] code is equivalent to the formally self-dual [22, 11, 7] code, and any linear [16, 8, 5] code is equivalent to the formally self-dual [16, 8, 5] code. In Section 4, we construct some optimal odd formally self-dual codes of lengths 18, 20 and 24. All extremal even formally self-dual codes of length up to 18 have been classified [1, 2, 5, 8, 11]. Thus our classification completes the classification of optimal formally self-dual codes of length up to 18 (Section 5).

2. Classification of Optimal Odd Formally Self-Dual Codes

2.1. The Highest Minimum Weight of Length up to 24

First we determine the highest minimum weight $d_O(n)$ of odd formally self-dual codes of length n in order to define optimal codes. The highest possible minimum weights are determined from known upper bounds for minimum weights of binary linear $[n, n/2]$ codes given in [3] except lengths 8, 18 and 24. The extended Hamming code is a unique [8, 4, 4] code. Thus $d_O(8) \le 3$. Any linear [18, 9, 6] code is equivalent to the extended quadratic residue code of length 18, which is even formally self-dual [11]. Thus $d_O(18) \le 5$. Since it is well known that a linear [24, 12, 8] code is equivalent to the extended Golay code, there is no odd formally self-dual $[24, 12, d]$ code with $d \ge 8$.

For length $n \le 24$, we list in Table 1 the highest minimum weights $d_O(n)$ of odd formally self-dual codes of length n. In the third column of the table, we list the number $N(n)$ of

Table 1. The highest minimum weights of length up to 24

Length n	$d_O(n)$	$N(n)$	$d_E(n)$	$d_L(n)$	$d_I(n)$	$d_{II}(n)$
2	1	1	—	2	2	
4	2	1	—	2	2	
6	3	1	2	3	2	
8	3	2	2	4	2	4
10	4	1	4	4	2	
12	4	5	4	4	4	
14	4	112	4	4	4	
16	5	1	4	5	4	4
18	5	≥2	6	6	4	
20	6	≥1	6	6	4	
22	7	1	6	7	6	
24	7	≥1	6	8	6	8

the inequivalent optimal odd formally self-dual codes of length n. To compare with $d_O(n)$ we also list the highest minimum weights $d_E(n)$, $d_L(n)$, $d_I(n)$ and $d_{II}(n)$ of even formally self-dual codes of length n, all linear $[n, n/2]$ codes, Type I and Type II self-dual codes of length n, respectively. The highest minimum weights of even formally self-dual codes are determined in [6] and [8]. Note that the even formally self-dual codes which we consider are not self-dual. All even formally self-dual codes of lengths 2 and 4 are self-dual [8]. All extremal Type I and Type II codes of length up to 32 have been classified (see [4]).

2.2. Classification for Lengths 2, 4 and 6

We start the classification of optimal odd formally self-dual codes.

- $n = 2$: Both odd formally self-dual codes with generator matrices $(1, 0)$ and $(0, 1)$ have weight enumerator $1 + y$.
- $n = 4$: A code with the following generator matrix

$$\begin{pmatrix} 1010 \\ 0111 \end{pmatrix}$$

  is an optimal odd formally self-dual [4, 2, 2] code with weight enumerator $1 + y^2 + 2y^3$. The automorphism group is the dihedral group of order 6. It is easy to see that any odd formally self-dual [4, 2, 2] code is equivalent to the above code.
- $n = 6$: A binary code is equivalent to a code with a generator matrix of the form (I, A). It can be easily seen that possible matrices A to generate odd formally self-dual [6, 3, 3] codes can become

$$A_1 = \begin{pmatrix} 110 \\ 101 \\ 011 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 110 \\ 101 \\ 111 \end{pmatrix}$$

  by permuting suitable rows and columns of A. Let C_1 and C_2 be the codes with generator matrices (I, A_1) and (I, A_2), respectively. Then it is so that $C_1^\sigma = C_2$ where $\sigma = (1, 2, 6)(3, 4)$. Thus there is a unique odd formally self-dual [6, 3, 3] code, up to equivalence. The weight enumerator is $1 + 4y^3 + 3y^4$ and the order of the automorphism group is 24.

2.3. Classification for Length 8

We found all odd formally self-dual [8, 4, 3] codes. This was done by considering 183 distinct 4×4 $(1, 0)$-matrices A with (I, A) generating the codes. Of these, 48 have weight enumerator

$$W_1 = 1 + 3y^3 + 7y^4 + 4y^5 + y^7$$

and the other codes have weight enumerator

$$W_2 = 1 + 4y^3 + 5y^4 + 4y^5 + 2y^6.$$

We verified by computer that all codes are equivalent for each weight enumerator. Thus an odd formally self-dual [8, 4, 3] code with W_1 is equivalent to the code with generator matrix

$$\begin{pmatrix} 1000 & 1100 \\ 0100 & 1010 \\ 0010 & 1001 \\ 0001 & 0111 \end{pmatrix}$$

and an odd formally self-dual code with W_2 is equivalent to the code with generator matrix

$$\begin{pmatrix} 1000 & 1100 \\ 0100 & 0110 \\ 0010 & 0011 \\ 0001 & 1001 \end{pmatrix}.$$

The orders of the automorphism groups of two codes are 24 and 8, respectively.

2.4. Classification for Length 10

We found all matrices A with (I, A) generating odd formally self-dual [10, 5, 4] codes. Any of the matrices A can become one of the following matrices

$$A_1 = \begin{pmatrix} 11100 \\ 11010 \\ 11001 \\ 10111 \\ 01111 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 11110 \\ 11101 \\ 11011 \\ 10111 \\ 01111 \end{pmatrix}$$

by permuting suitable rows and columns. Let C_1 and C_2 be the codes with generator matrices (I, A_1) and (I, A_2), respectively, then it is so that $C_1^\sigma = C_2$ where $\sigma = (3, 8, 10)(4, 6, 7)$. Thus there is a unique odd formally self-dual [10, 5, 4] code, up to equivalence. The weight enumerator is $1 + 10y^4 + 16y^5 + 5y^8$ and the order of the automorphism group is 1920.

2.5. Classification for Length 12

We describe how the optimal odd formally self-dual [12, 6, 4] codes C were classified. Every [12, 6] code is equivalent to a code with generator matrix of the form (I, A) where A is a 6×6 $(1, 0)$-matrix. Thus we only need to consider the set of 6×6 $(1, 0)$-matrices A, rather than the set of generator matrices.

The set of matrices A was constructed, row by row, using a back-tracking algorithm under the condition that the first row is (000111) since the minimum weight of C is 4. Permuting the rows of A gives rise to different generator matrices which generate equivalent codes. We consider only those matrices A which are smallest among all matrices obtained from A by permuting its rows, where the ordering involved is lexicographical on the binary integer corresponding to the rows of the matrix.

Then we found 9849 distinct matrices A (that is, 9849 distinct codes). The codes have the following five weight enumerators

$$W_1 = 1 + 6y^4 + 24y^5 + 16y^6 + 9y^8 + 8y^9,$$
$$W_2 = 1 + 8y^4 + 20y^5 + 14y^6 + 8y^7 + 7y^8 + 4y^9 + 2y^{10},$$
$$W_3 = 1 + 9y^4 + 18y^5 + 13y^6 + 12y^7 + 6y^8 + 2y^9 + 3y^{10},$$
$$W_4 = 1 + 10y^4 + 15y^5 + 16y^6 + 11y^7 + 5y^8 + 5y^9 + y^{11},$$
$$W_5 = 1 + 10y^4 + 16y^5 + 12y^6 + 16y^7 + 5y^8 + 4y^{10}.$$

The numbers of the codes with W_1, W_2, W_3, W_4 and W_5 are 30, 1422, 2088, 5472 and 837, respectively. We verified that all codes are equivalent for each weight enumerator. Some equivalences were verified by Magma. Thus there are exactly five inequivalent odd formally self-dual [12, 6, 4] codes. Let $C_{12,i}$ be the code with generator matrix (I, A_i) where

$$A_1 = \begin{pmatrix} 000111 \\ 001011 \\ 011101 \\ 101101 \\ 110011 \\ 111110 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 000111 \\ 001011 \\ 010101 \\ 101101 \\ 110011 \\ 111110 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 000111 \\ 001011 \\ 010101 \\ 101001 \\ 110011 \\ 111111 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 000111 \\ 001011 \\ 010101 \\ 101001 \\ 110001 \\ 111111 \end{pmatrix} \quad \text{and} \quad A_5 = \begin{pmatrix} 000111 \\ 001011 \\ 010011 \\ 100101 \\ 111001 \\ 111111 \end{pmatrix}$$

respectively. $C_{12,i}$ is an optimal odd formally self-dual code with weight enumerator W_i, $(i = 1, 2, 3, 4, 5)$. The orders of the automorphism groups of the five codes are 1152, 32, 24, 10 and 64, respectively.

2.6. *Classification for Length 14*

Similarly to length 12, we found all distinct 19020211 7×7 $(1, 0)$-matrices A such that the matrices (I, A) generate odd formally self-dual $[14, 7, 4]$ codes. The set of matrices A was constructed, row by row, using a back-tracking algorithm under the condition that the first row is (0000111) and by considering the lexicographical order on the rows. The codes are divided into the 29 distinct weight enumerators $W_1, W_2, \ldots, W_{29}$. To save space, the weight enumerators are listed in `http://www.math.nagoya-u.ac.jp/~koichi/data/`.

We complete the classification by listing all the inequivalent codes in Table 2 where the first column denotes the weight enumerator W, the second column gives the number N of the inequivalent codes with W, the third column lists the inequivalent codes F_i, the fourth

Table 2. Classification of codes of length 14

W	Numbers N	Codes	$\|Aut(F_i)\|$	Numbers T
W_1	1	F_1	384	612
W_2	1	F_2	8	38808
W_3	2	$F_{3,1}, F_{3,2}$	16, 2	213408
W_4	3	$F_{4,1}, F_{4,2}, F_{4,3}$	8, 2, 2	426960
W_5	1	F_5	1152	384
W_6	2	$F_{6,1}, F_{6,2}$	8, 80	62316
W_7	6	$F_{7,1}, \ldots, F_{7,6}$	2, 2, 2, 1, 1, 1	2015712
W_8	5	$F_{8,1}, \ldots, F_{8,5}$	4, 16, 16, 6, 2	459144
W_9	3	$F_{9,1}, F_{9,2}, F_{9,3}$	4, 1, 2	873504
W_{10}	14	$F_{10,1}, \ldots, F_{10,14}$	64, 4, 4, 32, 4, 4, 2, 2, 2, 2, 32, 8, 1, 2	2401524
W_{11}	2	$F_{11,1}, F_{11,2}$	168, 14	40224
W_{12}	2	$F_{12,1}, F_{12,2}$	16, 12	84576
W_{13}	18	$F_{13,1}, \ldots, F_{13,18}$	16, 4, 8, 4, 8, 4, 8, 4, 8, 1, 1, 1, 4, 4, 4, 4, 4, 2	3560472
W_{14}	1	F_{14}	2	281952
W_{15}	1	F_{15}	192	2925
W_{16}	3	$F_{16,1}, F_{16,2}, F_{16,3}$	1, 2, 6	1045440
W_{17}	12	$F_{17,1}, \ldots, F_{17,12}$	8, 32, 64, 32, 32, 16, 2, 4608, 768, 8, 32, 16	619491
W_{18}	3	$F_{18,1}, F_{18,2}, F_{18,3}$	4, 1, 2	1092672
W_{19}	15	$F_{19,1}, \ldots, F_{19,15}$	16, 6, 576, 4, 2, 2, 6, 6, 1, 2, 2, 1, 4, 16, 32	3468280
W_{20}	2	$F_{20,1}, F_{20,2}$	6, 1	774624
W_{21}	2	$F_{21,1}, F_{21,2}$	16, 16	84096
W_{22}	3	$F_{22,1}, F_{22,2}, F_{22,3}$	6, 2, 1	1191168
W_{23}	2	$F_{23,1}, F_{23,2}$	16, 16	88272
W_{24}	2	$F_{24,1}, F_{24,2}$	16, 12	110592
W_{25}	2	$F_{25,1}, F_{25,2}$	24, 16	78732
W_{26}	1	F_{26}	576	1376
W_{27}	1	F_{27}	1152	712
W_{28}	1	F_{28}	384	2232
W_{29}	1	F_{29}	322560	3

column gives the orders $|Aut(F_i)|$ of their automorphism groups and the fifth column lists the total number T of codes with W. Some equivalences were verified by Magma. To save space, generator matrices (I, G_i) of the inequivalent codes F_i listed in Table 2 are also listed in `http://www.math.nagoya-u.ac.jp/~koichi/data/`.

PROPOSITION 1. *All optimal odd formally self-dual codes are classified for length up to* 14.

Remark. The uniqueness of optimal odd formally self-dual codes of lengths 16 and 22 is given in Section 3.

3. Uniqueness of Linear Codes with Parameters [22, 11, 7] and [16, 8, 5]

3.1. Uniqueness of a Linear [22, 11, 7] Code

In this subsection, we show that there is a unique linear [22, 11, 7] code up to equivalence, and the code is equivalent to the optimal odd formally self-dual [22, 11, 7] code. The codewords of the minimum weight in the unique odd formally self-dual [22, 11, 7] code form a unique quasi-symmetric 2-(22, 7, 16) design with intersection numbers 1 and 3.

First we recall how to construct a linear [22, 11, 7] code from the extended Golay code which is a unique Type II self-dual [24, 12, 8] code. Let G_{24} be the extended Golay [24, 12, 8] code. Fix two coordinates (say, i_1 and i_2) of G_{24} then define

$$G'_{00}(i_1, i_2) = \{(x_1, \ldots, x_{24}) \in G_{24} \mid x_{i_1} = 0, x_{i_2} = 0\},$$

$$G'_{01}(i_1, i_2) = \{(x_1, \ldots, x_{24}) \in G_{24} \mid x_{i_1} = 0, x_{i_2} = 1\},$$

$$G'_{11}(i_1, i_2) = \{(x_1, \ldots, x_{24}) \in G_{24} \mid x_{i_1} = 1, x_{i_2} = 1\},$$

$$G'_{10}(i_1, i_2) = \{(x_1, \ldots, x_{24}) \in G_{24} \mid x_{i_1} = 1, x_{i_2} = 0\}.$$

We define $G_j(i_1, i_2)$ as the set obtained deleting the two coordinates i_1 and i_2 from $G'_j(i_1, i_2)$, $j = 00, 01, 11$ and 10. It is well-known that $G_{00}(i_1, i_2) \cup G_{10}(i_1, i_2)$ is a linear [22, 11, 7] code with the highest minimum weight among all [22, 11] codes.

LEMMA 2. *All codes $G_{00}(i_1, i_2) \cup G_{01}(i_1, i_2)$ and $G_{00}(i_1, i_2) \cup G_{10}(i_1, i_2)$ constructed from the extended Golay code by the above method are odd formally self-dual and equivalent. The weight enumerator is $W_{22} = 1 + 176y^7 + 330y^8 + 672y^{11} + 616y^{12} + 176y^{15} + 77y^{16}$. The automorphism group is the Mathieu group M_{22}.*

Proof. There is a unique self-dual [22, 11, 6] code, up to equivalence [10]. From the construction, $G_{00}(i_1, i_2) \cup G_{11}(i_1, i_2)$ is a unique self-dual [22, 11, 6] code G_{22} where $G_{00}(i_1, i_2)$ is the subcode consisting doubly-even weight codewords. Since the automorphism group of the extended Golay code G_{24} is the Mathieu group M_{24} which acts 5-fold transitively on the coordinates of G_{24}, $W_{G_{01}(i_1,i_2)} = W_{G_{10}(i_1,i_2)}$ where W_C denotes the weight enumerator of C. Note that $G_1(i_1, i_2) \cup G_3(i_1, i_2)$ is the shadow code of G_{22} (see [4] for the definition of shadow codes). It was also shown in [4] that $W_{G_{01}(i_1,i_2)} = W_{G_{10}(i_1,i_2)}$. Thus $G_{00}(i_1, i_2) \cup G_{01}(i_1, i_2)$ and $G_{00}(i_1, i_2) \cup G_{10}(i_1, i_2)$ are formally self-dual. Since the automorphism group of G_{24} is M_{24}, $G_{00}(i_1, i_2) \cup G_{01}(i_1, i_2)$ and $G_{00}(i'_1, i'_2) \cup G_{10}(i'_1, i'_2)$ $(1 \leq i_1, i_2, i'_1, i'_2 \leq 24)$ are equivalent. It follows from the construction that the weight enumerator W_{22} is $W_{G_{00}(i_1,i_2)} + W_{G_{01}(i_1,i_2)}$ and the automorphism group is the Mathieu group M_{22}. ■

Remark. By Theorems 3.3 and 3.4 in [9], the codewords of weight 7 in the above [22, 11, 7] code $G_0(i_1, i_2) \cup G_1(i_1, i_2)$ form a 3-design D_{22}. It follows from the weight enumerator W_{22} that any pair of two blocks in D_{22} intersects in 1 or 3 points. Thus D_{22} is also a quasi-symmetric 2-(22, 7, 16) design. By Theorem 3.3 in [12], there is a unique quasi-symmetric 2-(22, 7, 16) design with intersection numbers 1 and 3, up to isomorphism. This gives an alternative proof of the above lemma.

By the above lemma, there is at least one optimal odd formally self-dual [22, 11, 7] code. Similar to the proof of Theorem 3.3 in [12], we show the uniqueness of odd formally self-dual [22, 11, 7] codes.

PROPOSITION 3. *All odd formally self-dual* [22, 11, 7] *codes with weight enumerator W_{22} are equivalent.*

Proof. Suppose that F is an odd formally self-dual [22, 11, 7] code with weight enumerator W_{22}. Let F_0 and F_1 be the subsets of F consisting codewords of weights $\equiv 0$ and 3 (mod 4), respectively. We consider the following extension E of F

$$E = \{(0, 0, x) \mid x \in F_0\} \cup \{(1, 0, x) \mid x \in F_1\}.$$

It is easy to see that E is linear by considering the weight of each codeword. Thus E is a doubly-even self-orthogonal [24, 11, 8] code. Therefore $\langle E, \mathbf{1} \rangle$ is a Type II self-dual [24, 12, 8] code where **1** is the all-ones vector of length 24. The extended Golay code is a unique Type II self-dual [24, 12, 8] code and its automorphism group is M_{24}. Therefore the result follows. ∎

We checked by computer that all linear [22, 11, 7] codes have weight enumerator W_{22} (see also [7]). This was done by considering all 11×11 $(1, 0)$-matrices A such that the matrices (I, A) generate linear [22, 11, 7] codes. Thus we have the following corollary.

COROLLARY 4. *There is a unique linear* [22, 11, 7] *code, up to equivalence. The code is equivalent to the unique odd formally self-dual code with weight enumerator* W_{22}.

Of course, checking the weight enumerators of all linear [22, 11, 7] codes is easier than classifying such codes.

3.2. Uniqueness of a Linear [16, 8, 5] Code

A similar argument shows the uniqueness of a linear [16, 8, 5] code as follows. Let C_{16} be the linear code with generator matrix (I, A_{16}) where

$$A_{16} = \begin{pmatrix} 00001111 \\ 00110011 \\ 01010101 \\ 01101010 \\ 10010110 \\ 10101011 \\ 11011011 \\ 11101101 \end{pmatrix}.$$

The weight enumerator of C_{16} is $W_{16} = 1 + 24y^5 + 44y^6 + 40y^7 + 45y^8 + 40y^9 + 28y^{10} + 24y^{11} + 10y^{12}$. Thus C_{16} is an optimal odd formally self-dual code of length 16.

PROPOSITION 5. *All optimal odd formally self-dual* [16, 8, 5] *codes with weight enumerator* W_{16} *are equivalent.*

Proof. Let F be an odd formally self-dual [16, 8, 5] code with weight enumerator W_{16}. Let F_0 and F_1 be the subsets of F consisting codewords of even and odd weights, respectively.

Then $D = \langle E, \mathbf{1} \rangle$ is a linear $[18, 9, 6]$ code with weight enumerator $1 + 102y^6 + 153y^8 + 153y^{10} + 102y^{14} + y^{18}$ where $\mathbf{1}$ is the all-ones vector of length 18 and

$$E = \{(0, 0, x) \mid x \in F_0\} \cup \{(1, 0, x) \mid x \in F_1\}.$$

Thus D is an extremal even formally self-dual code of length 18. Simonis [11] showed that a linear $[18, 9, 6]$ code is equivalent to the extended qurdratic residue code of length 18. The automorphism group of the code is $PSL(2, 17)$ which acts doubly transitively on the coordinates of the code. Therefore the result follows. ∎

We verified that every linear $[16, 8, 5]$ code has weight enuerator W_{16}. This was done by considering all 8×8 $(1, 0)$-matrices A such that the matrices (I, A) generate linear $[16, 8, 5]$ codes. Thus we have the following corollary.

COROLLARY 6. *There is a unique linear* $[16, 8, 5]$ *code, up to equivalence. The code is equivalent to the unique optimal odd formally self-dual code.*

4. Construction of Optimal Odd Formally Self-Dual Codes

A (pure) double circulant code is a code with generator matrix of the form (I, R) where R is a circulant matrix. A double circulant code is formally self-dual. In this section, we construct optimal odd formally self-dual codes of lengths 18, 20 and 24.

We found all distinct double circulant codes with parameters $[18, 9, 5]$ and $[20, 10, 6]$. Our computer search shows that the exact numbers of inequivalent such codes are 2 and 1, respectively. Any double circulant $[18, 9, 5]$ code is equivalent to either $D_{18,1}$ or $D_{18,2}$ where the first rows of R for the two codes are (111010000) and (111110010), respectively. Any double circulant $[20, 10, 6]$ code is equivalent to D_{20} where the first row of R is (1111100100). This completes the classification of optimal double circulant odd formally self-dual codes of lengths 18 and 20.

For length 24, we consider the following generator matrix:

$$\begin{pmatrix} & 1 & \cdots & 1 \\ I & \vdots & R' & \\ & 1 & & \end{pmatrix}$$

where R' is the circulant matrix with first row (11101101000). This matrix generates an odd formally self-dual code with the weight enumerator

$$1 + 77y^7 + 506y^8 + 176y^9 + 616y^{11} + 1288y^{12} + 672y^{13} + 330y^{15} + 253y^{16} + 176y^{17} + y^{23}.$$

PROPOSITION 7. *The highest minimum weight of any odd formally self-dual codes of length up to* 24 *is known. The actual values are as given in Table 1.*

Table 3. Classification of optimal formally self-dual codes

Length n	$d(n)$	$N(n)$	References
2	1	1	Section 2
4	2	1	Section 2
6	3	1	Section 2
8	3	2	Section 2
10	4	2	[8], Section 2
12	4	7	[1], Section 2
14	4	121	[5], [2], Section 2
16	5	1	Section 3
18	6	1	[11]

5. Classification of Optimal Formally Self-Dual Codes

Recall that an *optimal* formally self-dual code has the highest minimum weight among even formally self-dual codes as well as odd formally self-dual codes. The classification of extremal even formally self-dual codes is known for length up to 18. In this paper, the classification of optimal odd formally self-dual codes has been given for length up to 16. These classifications imply the classification of optimal formally self-dual codes of length up to 18.

COROLLARY 8. *Optimal formally self-dual codes of length up to* 18 *are classified. The actual number* $N(n)$ *of the inequivalent optimal formally self-dual codes of length* n*, the highest minimum weight* $d(n)$ *and the references are as given in Table 3.*

Acknowledgment

The authors would like to thank T. Aaron Gulliver, David B. Jaffe, Masaaki Kitazume and Juriaan Simonis for their useful comments.

References

1. C. Bachoc, On harmonic weight enumerators of binary codes, *Designs, Codes and Cryptogr.,* Vol. 18 (1999) pp. 11–28.
2. K. Betsumiya, T. A. Gulliver, and M. Harada, On binary extremal formally self-dual even codes, *Kyushu J. Math.,* Vol. 53 (1999) pp. 421–430.
3. A. E. Brouwer and T. Verhoeff, An updated table of minimum-distance bounds for binary linear codes, *IEEE Trans. Inform. Theory,* Vol. 39 (1993) pp. 662–677.
4. J. H. Conway and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory,* Vol. 36 (1990) pp. 1319–1333.
5. J. E. Fields, P. Gaborit, W. C. Huffman, and V. Pless, On the classification of extremal even formally self-dual codes, *Designs, Codes and Cryptography,* Vol. 18 (1999) pp. 125–148.

6. M. Harada, The existence of a self-dual $[70, 35, 12]$ code and formally self-dual codes, *Finite Fields and Their Appl.*, Vol. 3 (1997) pp. 131–139.
7. D. B. Jaffe, Information about binary linear codes (server), University of Nebraska-Lincoln, USA, `http://www.math.unl.edu/djaffe/binary/codeform.html`.
8. G. Kennedy and V. Pless, On designs and formally self-dual codes, *Designs, Codes and Cryptogr.,* Vol. 4 (1994) pp. 43–55.
9. G. T. Kennedy and V. Pless, A coding theoretic approach to extending designs, *Discrete Math.,* Vol. 142 (1995) pp. 155–168.
10. V. Pless and N. J. A. Sloane, On the classification and enumeration of self-dual codes, *J. Combin. Theory Ser. A.,* Vol. 18 (1975) pp. 313–335.
11. J. Simonis, The $[18, 9, 6]$ code is unique, *Discrete Math.,* Vol. 106/107 (1992) pp. 439–448.
12. V. D. Tonchev, Quasi-symmetric designs and self-dual codes, *Europ. J. Combin.,* Vol. 7 (1986) pp. 67–73.