Classification of Extremal Formally Self-Dual Even Codes of Length 22

Masaaki Harada
Department of Mathematical Sciences
Yamagata University
Yamagata 990–8560, Japan
Email: mharada@sci.kj.yamagata-u.ac.jp

Patric R. J. Östergård
Department of Computer Science and Engineering
Helsinki University of Technology
P.O. Box 5400, 02015 HUT, Finland
Email: patric.ostergard@hut.fi

March 20, 2000

Abstract

Lengths 22 and 30 are so far the only open cases in the classification of extremal formally self-dual even codes. In this paper, a classification of the extremal formally self-dual even codes of length 22 is given. There are 41520 such codes. A variety of properties of these codes are investigated. In particular, new 2-$(22, 6, 5)$ designs are constructed from the codes.

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 of a codeword is the number of non-zero coordinates. The minimum weight of C is the smallest weight among all non-zero codewords of C. The minimum weight of a linear code equals the minimum distance of the code. An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d. Two binary linear codes 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 $W_C(y) = \sum_{i=0}^{n} A_i y^i$, where A_i is the number of codewords of weight i in C. A code with only even weights is called *even*.

The *dual* code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{F}_2^n | \ x \cdot y = 0 \text{ for all } y \in C\}$ where $x \cdot y$ denotes the standard inner-product of x and y. A *formally self-dual* code C is a code with the property that $W_C(y) = W_{C^\perp}(y)$. C is *isodual* if C and $C^\perp$ are equivalent and C is *self-dual* if $C = C^\perp$. A self-dual code is isodual and an isodual code is formally self-dual even.

The minimum weight d of a formally self-dual even code of length n is bounded by $d \leq 2\lfloor n/8 \rfloor + 2$. A formally self-dual even code of length n and minimum weight $2\lfloor n/8 \rfloor + 2$ is called *extremal*. Ward [16] showed that extremal self-dual codes of length n exist if and only if $n = 2, 4, 6, 8, 12, 14, 22$ and 24.

Recently formally self-dual even codes have received a great deal of interest (see, for example, [2], [3], [5], [6], [7] and [9]). Of most interest are *extremal* formally self-dual even codes. In particular, it is known that there are extremal formally self-dual even codes which are not self-dual only for lengths 6, 10, 12, 14, 18, 20, 22, 28 and 30. All such codes have been classified for lengths 6, 10, 12, 14, 18, 20 and 28 (see Table 1). In this paper, we give a classification of extremal formally self-dual even codes of length 22. This completes the classification of all extremal formally self-dual even codes except length 30.

In Section 2, previous results on classifying extremal formally self-dual even codes are surveyed. Our approach for classifying such codes of length 22 is discussed in Section 3. In this classification, 41520 codes are obtained. Properties of these codes are investigated in Section 4. In Section 5, we investigate designs in the codewords of a fixed weight in these codes. In particular, new 2-$(22, 6, 5)$ designs are constructed. In Section 6, the smallest covering radius of extremal formally self-dual even codes are studied.

2 Known Classification Results

We now describe the known results concerning the existence and classification of extremal formally self-dual even codes.

As described above, extremal self-dual codes of length n exist if and only if $n = 2$, 4, 6, 8, 12, 14, 22 and 24. For each length, such a code is unique. Simonis [15] showed that the extended quadratic residue code of length 18 is the unique $[18, 9, 6]$ code, up to equivalence. The extended quadratic residue code is formally self-dual even. In [9], all formally self-dual even codes of length up to 8 and extremal formally self-dual even codes of length 10 were classified. Extremal formally self-dual even codes of length 12 were classified in [2]. The classification of extremal formally self-dual even codes of length 14 were given in [3] and [5] by different methods, independently. Jaffe [8] proved that there is a unique linear $[28, 14, 8]$ code. This code is extremal formally self-dual even. Recently, Fields, Gaborit, Huffman and Pless [6] gave the classification of extremal formally self-dual even codes of length 20 applying the method in [5] to length 20. For length 22, they stopped the classification after finding over 1000 inequivalent extremal formally self-dual even codes.

All extremal formally self-dual even codes of lengths 2, 4, 8 and 24 are actually self-dual. Recently, Zhang [17] showed that the extremal weight enumerator contains a negative coefficient for lengths $8i$ ($i \geq 4$), $8i + 2$ ($i \geq 5$), $8i + 4$ ($i \geq 6$) and $8i + 6$ ($i \geq 7$). There is no linear $[n, n/2, d \geq 2\lfloor n/8 \rfloor + 2]$ code for $n = 16$, 26, 34, 36, 38, 44, 46 and 54 (see [4]). Therefore there are extremal formally self-dual even codes which are not self-dual only for lengths 6, 10, 12, 14, 18, 20, 22, 28 and 30.

Table 1: Classification of Extremal Formally Self-Dual Even Codes

Length	N_{SD}	N_{FSD}	$N_{FSD,I}$	$N_{FSD,DC}$	References
2	1	0	0	0	[9]
4	1	0	0	0	[9]
6	1	1	1	1	[9]
8	1	0	0	0	[9]
10	0	1	1	1	[9]
12	1	2	2	2	[2]
14	1	9	9	4	[3], [5]
16	0	0	0	0	[4]
18	0	1	1	1	[15]
20	0	7	7	3	[6]
22	1	41519	2821	9	Sections 3 and 4
24	1	0	0	0	[12]
26	0	0	0	0	[4]
28	0	1	1	1	[8]
30	0	≥ 6	≥ 6	6	[7]
≥ 32	0	0	0	0	[4], [17]

The known results on the classification of extremal formally self-dual even codes are summarized in Table 1. In this table, N_{SD} denotes the number of inequivalent extremal self-dual codes, N_{FSD} denotes the number of inequivalent extremal formally self-dual even codes that are not self-dual, and $N_{FSD,I}$ denotes the number of inequivalent isodual codes that are not self-dual. The final column gives the references for the classification of extremal formally self-dual even codes that are not self-dual. This table also contains the results presented in this paper.

Double circulant codes are divided into two types, namely pure and bordered. A code having a generator matrix of the form $[\ I \mid R_n\ ]$ is called pure double circulant, where R_n is an n by n circulant matrix. The generator matrix of a bordered double circulant code of length $2n+2$ has the form

$$\left[\begin{array}{ccc} & \varepsilon & 1 \ \cdots \ 1 \\ & 1 & \\ I & \vdots & R_n \\ & 1 & \end{array}\right],$$

where $\varepsilon = ((-1)^n + 1)/2$. Double circulant codes are isodual codes. All extremal formally self-dual even double circulant codes which are not self-dual have been classified by Gulliver and the first author [7]. The number of inequivalent such codes, $N_{FSD,DC}$, is also given in Table 1.

3 Classification of Length 22

In the classification, we make use of existing software for classifying linear codes, developed by the second author [11]. We shall here describe this approach briefly, in particular explaining the special considerations that we need to take into account for formally self-dual even codes.

The approach in [11] and here is to construct the parity check matrices of the $[n, k, d \geq d']$ codes by lengthening the $[n-1, k-1, d \geq d']$ codes in all possible ways. Lengthening is done by adding a column to the parity check matrix. This is done repeatedly starting from the code of length $n-k$ with parity check matrix $[\ I\ ]$. The codes constructed must have minimum weight at least d. Moreover, only one copy of equivalent codes is accepted. Equivalence tests of codes therefore have a central role in this procedure. For details of our algorithm for equivalence tests of linear codes, the reader is referred to [11].

It is well known that a linear code always has an equivalent code with parity check matrix $[\ I \mid A\ ]$; the codes obtained using the previously described approach are all of this type. We shall therefore restrict our consideration to the A part of the parity check matrix.

The A part of a parity check matrix of a formally self-dual even $[22, 11, 6]$ code has the following properties: Because the minimum weight is 6, every row and column has weight at least 5. As the code is even, the weight of every row and column is odd. Finally, by the Gleason theorem (see [13]), we know that the weight enumerator of the code is

$$1 + 77y^6 + 330y^8 + 616y^{10} + 616y^{12} + 330y^{14} + 77y^{16} + y^{22}. \tag{1}$$

These further requirements were implemented in the existing software. When recursively building up A, one column at a time, for the first few columns it was checked that the codes were even and with minimum weight at least 6. For the seventh column onwards, only matrices A with at least $(p-6)$ 1s in every row, where $7 \leq p \leq 11$ is the number of the column, were accepted. In this way, we were able to get to eight columns, with 345761 inequivalent matrices. Due to the large number of matrices to be expected after adding one more column, the strategy had to be changed at this point.

Starting from all aforementioned 345761 matrices, we added two more columns in all possible ways, so that the columns that were added had an odd number of 1s, the codes had minimum weight 6, and the requirements on the rows were fulfilled. The eleventh and final column is then uniquely determined, as all rows must have odd weight. As a last step, the weight enumerator was calculated for the final code, and the code was accepted and saved if it coincided with (1). No equivalence tests were carried out. This calculation was distributed over a network of computers.

In this way, we ended up with 22,346,601 codes, which were all formally self-dual even $[22, 11, 6]$ codes, but many of which were equivalent. Going through all these codes, it turned out that there are 41520 inequivalent formally self-dual even $[22, 11, 6]$ codes. Several months of CPU time on 233–500 MHz PCs were needed for the complete classification.

Proposition 1 *There are* 41520 *inequivalent extremal formally self-dual even* $[22, 11, 6]$ *codes, one of which is the unique extremal self-dual code.*

As there are too many codes to list them in print, we make them available electronically (at `http://www.tcs.hut.fi/~pat/fsd22.html`). We give only six examples $C_{22,i}$ $(i = 1, 2, \ldots, 6)$ with generator matrices $[\ I \mid A_i\ ]$ where

$$A_1 = \begin{bmatrix} 11111000000 \\ 11100110000 \\ 11010101000 \\ 10110100100 \\ 11001010010 \\ 10001001110 \\ 10001110001 \\ 11000001101 \\ 01100001011 \\ 10110010111 \\ 01011111111 \end{bmatrix}, \ A_2 = \begin{bmatrix} 11111000000 \\ 11100110000 \\ 11010101000 \\ 10110100100 \\ 11001010010 \\ 10001001110 \\ 10001110001 \\ 11000001101 \\ 00100011011 \\ 01011010111 \\ 11110101111 \end{bmatrix} \ A_3 = \begin{bmatrix} 11111000000 \\ 11100110000 \\ 11010101000 \\ 10110100100 \\ 11001010010 \\ 10001001110 \\ 10001110001 \\ 10100001101 \\ 10000011011 \\ 00110000111 \\ 01011111111 \end{bmatrix},$$

$$A_4 = \begin{bmatrix} 11111000000 \\ 11100110000 \\ 11010101000 \\ 10101100100 \\ 10011100010 \\ 11100011110 \\ 00100111001 \\ 00001110101 \\ 11011001011 \\ 10001000111 \\ 10011111111 \end{bmatrix}, \ A_5 = \begin{bmatrix} 11111000000 \\ 11100110000 \\ 11010101000 \\ 10001011100 \\ 10111011010 \\ 01101000110 \\ 10101111001 \\ 01100010101 \\ 00111110011 \\ 11010100111 \\ 01001011111 \end{bmatrix} \ \text{and } A_6 = \begin{bmatrix} 11111000000 \\ 11100110000 \\ 11010101000 \\ 10001011100 \\ 10111011010 \\ 01101000110 \\ 10101111001 \\ 01000110101 \\ 00011010011 \\ 11010100111 \\ 01001011111 \end{bmatrix},$$

respectively. $C_{22,1}$, $C_{22,2}$ and $C_{22,3}$ have small automorphism groups of orders $1, 2$ and 3, respectively. $C_{22,4}$, $C_{22,5}$ and $C_{22,6}$ have large automorphism groups of orders 3840, 768 and 960, respectively (see Table 2 for the orders of all automorphism groups).

By Proposition 1, we have the following corollary and problem.

Corollary 2 *Extremal formally self-dual even codes of all lengths except* 30 *are classified.*

Problem. Classify extremal formally self-dual even codes of length 30.

4 Some Properties of the Codes

Having classified the extremal formally self-dual even codes of length 22, we shall now investigate them by calculating some central parameters. Some of these parameters were calculated in [6] for 1000 of the codes that they found.

4.1 Isoduality

As pointed out in [3, Corollary 4], all extremal formally self-dual even codes are isodual for lengths up to 18. The first examples of extremal formally self-dual even codes of length 22 which are not isodual were found in [3]. Later, more examples of such codes were given in [6]. For length 20, all extremal formally self-dual even codes are isodual [6]. Our computer search shows that only 2822 of the extremal formally self-dual even codes of length 22 are isodual. In our examples, the codes $C_{22,i}$ with $i \neq 2$ are isodual.

4.2 Automorphism Groups

One important property of a code is its automorphism group. The orders of the automorphism groups of the classified codes are displayed in Table 2. The largest group of order 887040 is the Mathieu group M_{22}, that is, the automorphism group of the unique self-dual code. The 1000 codes found in [6] have automorphism groups of orders ≤ 24. Table 2 shows that there are codes with larger automorphism groups, for example, $C_{22,4}$, $C_{22,5}$ and $C_{22,6}$.

There has been interest recently in self-dual codes with trivial automorphism groups (cf. [13, Section 13.3]). It is an open problem to determine the smallest length for which there is a binary self-dual code with a trivial automorphism group. One may consider the analogue problem for extremal formally self-dual even codes. From the classification of such codes, all such codes have non-trivial automorphism groups for length up to 20. From Table 2, there are many extremal formally self-dual even codes with trivial automorphism groups for length 22. An example of codes with a trivial automorphism group is $C_{22,1}$.

Table 2: Automorphism Groups of Codes

$\lvert Aut(C)\rvert$	1	2	3	4	5	6	7	8	10	11	12	14	16
Number of codes	40134	1237	10	64	12	14	2	9	10	2	2	2	3

$\lvert Aut(C)\rvert$	20	22	24	32	64	96	256	768	960	3840	887040
Number of codes	4	1	1	3	4	1	1	1	1	1	1

Table 3: Statistics for the Hull

$\dim(C \cap C^{\perp})$	1	3	5	7	9	11
Number of codes	17046	23308	1134	28	3	1

4.3 Dimension of the Hull

Another interesting parameter is the dimension of the hull. The hull of a code C is the subspace $C \cap C^{\perp}$. In [6] it was known that among the classified codes, there are codes for which the dimension of the hull is 1, 3, 5 and 11. Other possibilities for the dimension are 7 and 9 according to [5, Corollary 6.2].

Checking the hull of the classified codes reveals that there are indeed codes that have a hull of dimensions 7 and 9. The statistics for the dimensions of the hull are given in Table 3.

5 2-(22, 6, 5) Designs

In this section, we investigate designs in extremal formally self-dual even codes of length 22 (see, for example, [10] for definitions of designs).

By the Assmus-Mattson theorem, if C is an extremal formally self-dual even code of length n, then the codewords of a fixed weight in C form a 3-design if $n \equiv 0 \pmod 8$, a 2-design if $n \equiv 2 \pmod 8$ and a 1-design if $n \equiv 4 \pmod 8$. It is not explained by the Assmus-Mattson theorem whether the codewords of a fixed weight form a design for length $n \equiv 6 \pmod 8$. However, it is well known that the codewords of a fixed weight in the unique self-dual code form a 3-design since the Mathieu group M_{22} is the automorphism group.

We checked all formally self-dual codes to see if the codewords of a fixed weight form a t-design. The numbers of codes containing t-designs in the codewords of the minimum weight are listed in Table 4 where $t = 1, 2, 3$. Our computer search also shows that if the

Table 4: $1,2$ and 3-Designs

t-designs	$t=3$	$t=2$	$t=1$
Number of codes	1	3	974

codewords of the minimum weight form a t-design then the codewords of a fixed weight form a t-design.

From the table, the self-dual code is the unique code having 3-designs. Only the self-dual code, $C_{22,5}$ and $C_{22,6}$ contain 2-designs. Note that the automorphism groups of $C_{22,5}$ and $C_{22,6}$ do not act on the coordinates transitively.

Proposition 3 *There are three inequivalent extremal formally self-dual even codes of length* 22 *such that the codewords of a fixed weight form a* 2*-design.*

According to [10, Table 1.28], only one example of a 2-$(22,6,5)$ design is known. It is well known that the 2-$(22,6,5)$ design in the unique self-dual code is a quasi-symmetric design with intersection numbers 0 and 2. There is a unique such design (cf. [14, Table 37.22]).

Since the three codes are inequivalent and the codewords of weight 6 generate the codes, the three 2-$(22,6,5)$ designs are not isomorphic. Moreover the two designs in $C_{22,5}$ and $C_{22,6}$ are not quasi-symmetric.

Therefore we have the following:

Corollary 4 *There are at least three non-isomorphic* 2-$(22,6,5)$ *designs. There are at least two non-isomorphic* 2-$(22,6,5)$ *designs which are not quasi-symmetric.*

6 Smallest Covering Radius of Extremal Formally Self-Dual Even Codes

In this section, we study the smallest covering radius of extremal formally self-dual even codes.

The covering radius $R(C)$ of a code C is the smallest integer R such that spheres of radius R around codewords of C cover the space $\mathbb{F}_2^n$. For linear codes, the covering radius is the largest weight of all the coset leaders of the code. The covering radius is a basic and important geometric parameter of a code. A basic question concerning the covering radius is to find a code with the smallest covering radius for given parameters. Assmus and Pless [1] gave various bounds on the covering radius and investigated the covering radii of extremal doubly-even self-dual codes.

Proposition 5 (Assmus and Pless [1]) *If C is an even $[n,k]$ code then*

$$\sum_{0 \le 2i \le R(C)} \binom{n}{2i} \ge 2^{n-k-1} \quad \textit{and} \quad \sum_{1 \le 2i+1 \le R(C)} \binom{n}{2i+1} \ge 2^{n-k-1}.$$

In order to determine the smallest covering radius of extremal formally self-dual even codes of lengths except 30 and give a bound on the smallest covering radius of length 30, we computed the covering radii of some of the known codes. The numbers of codes of length 22 with each covering radius are listed in Table 5. Note that the unique code with covering radius 7 is the self-dual code. $C_{22,1}$, $C_{22,2}$ and $C_{22,3}$ have covering radius 5, and $C_{22,4}$, $C_{22,5}$ and $C_{22,6}$ have covering radius 6.

Table 5: Covering Radii of Length 22

$R(C)$	5	6	7
Number of codes	41509	11	1

In Table 6, the smallest covering radius R_n of extremal formally self-dual even codes of length n is listed. The lower bounds obtained from Proposition 5 are given in the third column and examples of codes with the indicated covering radius are given in the final column in the table. From the table, we have the following:

Proposition 6 *The smallest covering radii of extremal formally self-dual even codes of all lengths except* 30 *are determined.*

Let C be an extremal formally self-dual even code of length 30. By Proposition 5, $R(C) \ge 5$. $C_{30,1}$ in [7] has covering radius 6. Thus the smallest covering radius of extremal formally self-dual even codes of length 30 is 5 or 6.

Problem. Determine the smallest covering radius of extremal formally self-dual even codes of length 30.

References

[1] E.F. Assmus, Jr. and V. Pless, On the covering radius of extremal self-dual codes, *IEEE Trans. Inform. Theory* **29** (1983) 359–363.

[2] C. Bachoc, On harmonic weight enumerators of binary codes, *Des. Codes Cryptogr.* **18** (1999) 11–28.

Table 6: Smallest Covering Radii of Extremal Formally Self-Dual Even Codes

Length n	R_n	Lower bound	Examples
6	2	2	the unique code
10	3	3	the unique code
12	3	3	C_1 in [2]
14	3	3	C_1 in [3]
18	4	4	the unique code
20	4	4	$fsd20\_2b, fsd20\_2d, fsd20\_4$ in [6]
22	5	4	41509 codes, e.g., $C_{22,1}, C_{22,2}, C_{22,3}$
28	6	5	the unique code
30	5 or 6	5	$C_{30,1}$ in [7] ($R(C_{30,1}) = 6$)

[3] K. Betsumiya, T.A. Gulliver and M. Harada, On binary extremal formally self-dual even codes, *Kyushu J. Math.* **53** (1999) 421–430.

[4] A.E. Brouwer, "Bounds on the size of linear codes," in Handbook of Coding Theory, V.S. Pless and W.C. Huffman (Editors), Elsevier, Amsterdam 1998, pp. 295–461.

[5] J.E. Fields, P. Gaborit, W.C. Huffman and V. Pless, On the classification of extremal even formally self-dual codes, *Des. Codes Cryptogr.* **18** (1999) 125–148.

[6] J.E. Fields, P. Gaborit, W.C. Huffman and V. Pless, On the classification of extremal even formally self-dual codes of lengths 20 and 22, (preprint).

[7] T.A. Gulliver and M. Harada, Classification of extremal double circulant formally self-dual even codes, *Des. Codes Cryptogr.* **11** (1997) 25–35.

[8] D.B. Jaffe, Optimal binary linear codes of length ≤ 30, *Discrete Math.*, (to appear).

[9] G. Kennedy and V. Pless, On designs and formally self-dual codes, *Des. Codes Cryptogr.* **4** (1994) 43–55.

[10] R. Mathon and A. Rosa, "2-(v, k, λ) designs of small order," in *The CRC Handbook of Combinatorial Designs*, C.J. Colbourn and J.H. Dinitz (Eds.), CRC Press, Boca Raton 1996, pp. 3–41.

[11] P.R.J. Östergård, Classifying subspaces of Hamming spaces, (submitted).

[12] V. Pless, On the uniqueness of the Golay codes, *J. Combin. Theory* **5** (1968) 215–228.

[13] E. Rains and N.J.A. Sloane, "Self-dual codes," in *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman (Eds.), Elsevier, Amsterdam 1998, pp. 177–294.

[14] M.S. Shrikhande, "Quasi-symmetric designs," in *The CRC Handbook of Combinatorial Designs*, C.J. Colbourn and J.H. Dinitz (Eds.), CRC Press, Boca Raton 1996, pp. 430–434.

[15] J. Simonis, The $[18, 9, 6]$ code is unique, *Discrete Math.* **106/107** (1992) 439–448.

[16] H.N. Ward, A restriction on the weight enumerators of a self-dual code, *J. Combin. Theory Ser. A* **21** (1976) 253–255.

[17] S. Zhang, On the nonexistence of extremal self-dual codes, *Discrete Appl. Math.* **91** (1999) 277–286.