

The Search for the $[24k, 12k, 4k + 4]$ Extremal Type II Code

Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18510
USA
doughertys1@scranton.edu

November 29, 2006

Abstract

We discuss the difficult question of the existence of a Type II $[24k, 12k, 4k + 4]$ Type II self-dual code especially the first open case when $k = 3$ and examine several possible paths to a solution.

1 Introduction

We describe the very difficult problem of finding extremal $[24k, 12k, 4k + 4]$ Type II codes. The first open case is the existence of a $[72, 36, 16]$ Type II code. This problem was first introduced in 1973 by N.J.A. Sloane in [31] and a \$10 prize was offered. Recently the author offered a prize of \$100 for a proof of the existence of the code and M. Harada offered a prize of \$200 for a non-existence proof.

For any undefined terms from coding theory see MacWilliams and Sloane's book [24]. We shall attempt to maintain consistency with the notation in this book. For a full description (and an extensive bibliography) of the theory of self-dual codes see the chapter on self-dual codes by Rains and Sloane in the Handbook of Coding Theory [30]. For a recent update on the study of binary self-dual codes see [10].

We begin with some definitions. A linear binary $[n, k, d]$ code is a k -dimensional subspace of \mathbb{F}_2^n with minimum weight d . A non-linear code is simply a set of vectors. We consider only binary codes, specifically self-dual codes, namely those codes C for which $C = C^\perp$, where C^\perp denotes the orthogonal under the standard inner-product.

If a self-dual code has only vectors of doubly-even weight then we say that the code is a doubly-even code, otherwise we say that it is a singly-even code. Doubly-even self-dual binary codes are said to be Type II codes and singly-even self-dual codes are said to be Type I codes. We denote the weight enumerator by:

$$W_C(x, y) = \sum A_i x^{n-i} y^i$$

where there are A_i vectors of weight i in C . When recording a weight enumerator we shall set $x = 1$, and when it is symmetric we will only show half.

2 Weight enumerators of self-dual codes

2.1 Invariant Theory

A detailed description of the material in this section can be found in [24].

If C is a self-dual code then the weight enumerator is held invariant by the MacWilliams relations and hence by the following matrix:

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

If the code is doubly-even, then it is also held invariant by the following matrix:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

The group $G = \langle G, A \rangle$ has order 192. The series $\Phi(\lambda) = \sum a_i \lambda^i$ where there are a_i independent polynomials held invariant by the group G . Next we apply the classic theorem of Molien.

Theorem 2.1 (Molien) *For any finite group G of complex m by m matrices, $\Phi(\lambda)$ is given by*

$$(1) \quad \Phi(\lambda) = \frac{1}{|G|} \sum_{A \in G} \frac{1}{\det(I - \lambda A)}$$

where I is the identity matrix.

For our group G we get

$$(2) \quad \Phi(\lambda) = \frac{1}{(1 - \lambda^8)(1 - \lambda^{24})} = 1 + \lambda^8 + \lambda^{16} + 2\lambda^{24} + 2\lambda^{32} + \dots$$

The generating invariants can be found. Specifically, we have:

$$(3) \quad W_1(x, y) = x^8 + 14x^4y^4 + y^8$$

and

$$(4) \quad W_2(x, y) = x^4y^4(x^4 - y^4)^4$$

Then we have the well known Gleason's Theorem first proven in [13].

Theorem 2.2 (Gleason) *The weight enumerator of an Type II self-dual code is a polynomial in $W_1(x, y)$ and $W_2(x, y)$, i.e. if C is a Type II code then $W_C(x, y) \in \mathbb{C}[W_1(x, y), W_2(x, y)]$.*

It follows that if C is a Type II $[n, k, d]$ code then

$$(5) \quad d \leq 4 \lfloor \frac{n}{24} \rfloor + 4$$

Codes meeting this bound are called extremal. We investigate those with parameters $[24k, 12k, 4k + 4]$. It is not known whether these codes exist until $24k \geq 3720$ at which a coefficient becomes negative.

Using this theorem it is then easy to determine the weight enumerator for a putative $[72, 36, 16]$ Type II code. It is given in Table 1.

Table 1: The Weight Enumerator for a Type II $[72, 36, 16]$ Code and its $[70, 35, 14]$ Child

C_i	i
1	0, 72
249849	16, 56
18106704	20, 52
462962955	24, 48
4397342400	28, 44
16602715899	32, 40
25756721120	36
D_i	i
1	0, 70
11730	14, 56
150535	16, 54
1345960	18, 52
9393384	20, 50
49991305	22, 48
204312290	24, 46
650311200	26, 44
1627498400	28, 42
3221810284	30, 40
5066556495	32, 38
6348487600	34, 36

2.2 Shadows

Shadow codes were introduced by Conway and Sloane in [6].

Let C be a self-dual code with C_0 the subcode of doubly-even vectors.

Lemma 2.3 *The subcode C_0 is linear and of codimension 1.*

Proof. If v and w are doubly-even vectors then

$$(6) \quad wt(v + w) = wt(v) + wt(w) - 2|v \wedge w| \equiv 0 \pmod{4},$$

since both $wt(v)$ and $wt(w)$ are $0 \pmod{4}$ and $|v \wedge w|$ is even since the vectors are orthogonal. Then the map $\psi : C \rightarrow \mathbb{F}_2$ with $\psi(c) = 0$ if it is doubly-even and 1 if it is singly even, is linear and C_0 is the kernel, which gives that $2|C_0| = |C|$ and so the code is of codimension 1. \square

Then $C_0^\perp = C_0 \cup C_1 \cup C_2 \cup C_3$ with $C = C_0 \cup C_2$. Let $S = C_1 \cup C_3$ be the shadow of C with respect to the subcode C_0 . Note that the shadow is a non-linear code. In [11] **shadow extremal** codes are defined to be extremal self-dual codes whose shadow has the highest possible minimum weight for each length. If C_0 is the subcode of doubly-even vectors when C is a singly-even code, then it is easy to determine the weight enumerator of C_0 from the weight enumerator of C , namely:

$$(7) \quad W_{C_0}(x, y) = \left(\frac{1}{2}\right)(W_C(x, y) + W_C(x, iy))$$

where i is the complex number with $i^2 = -1$. Then using the MacWilliams identities it is easy to determine the weight enumerator of the shadow. Throughout this correspondence it will be assumed that C_0 is the subcode of doubly-even vectors if no subcode is specified. The next lemma is due to Conway and Sloane [6].

Lemma 2.4 *Let C be a Type I self-dual code with S its shadow then*

$$(8) \quad W_S(x, y) = W_C\left(\frac{x+y}{\sqrt{2}}, \frac{i(x-y)}{\sqrt{2}}\right).$$

Proof. Let T be the action of the MacWilliams transform.

$$\begin{aligned} W_S(x, y) &= W_{C_0^\perp}(x, y) - W_C(x, y) \\ &= \frac{1}{|C_0|} T \cdot W_{C_0}(x, y) - W_C(x, y) \\ &= \frac{1}{2|C_0|} T \cdot (W_C(x, y) + W_C(x, iy)) - W_C(x, y) \\ &= \frac{1}{|C|} T \cdot W_C(x, y) + \frac{1}{|C|} T \cdot W_C(x, iy) - W_C(x, y) \\ &= \frac{1}{|C|} T \cdot W_C(x, iy) \end{aligned}$$

□

Conway and Sloane show, using Gleason's theorem, how to construct the weight enumerators of the code and its shadow.

Theorem 2.5 (Conway and Sloane [6]) *The weight enumerator of a self-dual code of length n by Gleason's theorem is given by:*

$$W_C(x, y) = \sum_{j=0}^{\lfloor \frac{n}{8} \rfloor} a_j (x^2 + y^2)^{\frac{n}{2} - 4j} (x^2 y^2 (x^2 - y^2)^2)^j$$

and the weight enumerator of the shadow with C_0 as the subcode of doubly-even vectors is given by:

$$W_S(x, y) = \sum_{j=0}^{\lfloor \frac{n}{8} \rfloor} (-1)^j a_j 2^{\frac{n}{2} - 6j} (xy)^{\frac{n}{2} - 4j} (x^4 - y^4)^{2j}$$

In [4] Brualdi and Pless show how to use these codes to produce larger self-dual codes from existing self-dual codes. These ideas were further investigated in [7]. The following theorem shows how this is accomplished.

Theorem 2.6 (Brualdi and Pless [4]) *Let C be a self-dual code of length n , C_0 be any subcode of codimension 1, and S be the shadow with respect to that subcode, with $C_0^\perp = C_0 \cup C_1 \cup C_2 \cup C_3$ as described above. Then if $\mathbf{j} \notin C_0$, where \mathbf{j} is the all-one vector, the code*

$$C' = (0, 0, C_0) \cup (1, 1, C_2) \cup (1, 0, C_1) \cup (0, 1, C_3)$$

is a self-dual code of length $n + 2$ with weight enumerator:

$$W_{C'} = x^2 W_{C_0}(x, y) + y^2 W_{C_2}(x, y) + xy W_S(x, y)$$

If $\mathbf{j} \in C_0$ then the code

$$C' = (0, 0, 0, 0, C_0) \cup (1, 1, 0, 0, C_2) \cup (1, 0, 1, 0, C_1) \cup (0, 1, 1, 0, C_3)$$

is self-orthogonal and the code $C^* = \langle v, C' \rangle$, where $v = (1, 1, 1, 1, 0, \dots, 0)$, is a self-dual code of length $n + 4$ with weight enumerator:

$$(x^4 + y^4) W_{C_0}(x, y) + (2x^2 y^2) (W_{C_1}(x, y) + W_{C_2}(x, y) + W_{C_3}(x, y))$$

In either case we refer to the larger code as the parent code and the smaller code as the child.

Let C be a self-dual code of length $n + 2$. We can take as a generator matrix, a matrix of the following form:

$$(I, G)$$

where I is the identity matrix. It follows that we can then take a generator matrix to be

$$\begin{pmatrix} 0 & 0 & H_1 \\ 0 & 0 & H_2 \\ 0 & 0 & H_3 \\ & & \cdot \\ & & \cdot \\ & & \cdot \\ 0 & 0 & H_{\frac{n}{2}-1} \\ 1 & 1 & v \\ 0 & 1 & u \end{pmatrix}$$

where the matrix H with rows $H_1, \dots, H_{\frac{n}{2}-1}$ generates a self-orthogonal code D_0 which is of codimension one in the self-dual $[n, \frac{n}{2}]$ code D generated by H and v — provided C does not have minimum weight 2.

We have that $[u, v] = 1$ and also that $[u, H_i] = 0$ giving that C is formed by the shadow construction from D , i.e. that C is the parent of D . This gives the following:

Theorem 2.7 *If C is a self-dual code of length $n + 2$ with minimum weight greater than 2, then for some self-dual code D of length n , we have that C is the parent of D .*

Assume that C is a doubly-even self-dual code of length $n + 2$ and consider the above matrix. It is clear that the vectors in the matrix H are doubly-even and that v is singly-even, which gives the following:

Corollary 2.8 *If C is a doubly-even self-dual code of length $n + 2$, then for some self-dual code D of length n , C is the parent of D with*

$$C = (0, 0, D_0) \cup (1, 1, D_2) \cup (1, 0, D_1) \cup (0, 1, D_3)$$

where D_0 is the subcode of doubly-even vectors of D .

Denote the minimum weight of a code E by $m(E)$. Let z be a minimum weight vector of D , then z is either in D_0 or in D_2 . If $z \in D_0$ then $(0, 0, z)$ is a vector in C giving that $m(C) \leq m(D)$. If $z \in D_2$ then $(1, 1, z)$ is a vector in C giving that $m(C) \leq m(D) + 2$.

Theorem 2.9 *If α is the highest minimum weight for a self-dual code of length n then $\alpha + 2$ is the highest possible minimum weight of a self-dual code of length $n + 2$.*

Proof. If C is a code of length $n + 2$ then by the previous theorem we have that C is the parent of a some self-dual code D of length n assuming, of course, that the minimum weight of C is greater than 2. By the above the best attainable is $m(C) \leq m(D) + 2$ and since the maximum value $m(D)$ can have is α , then $m(C) \leq \alpha + 2$. \square

3 Extremal doubly-even codes of length a multiple of 24

Let C be a binary doubly-even self-dual $[72, 36, 16]$ code. The existence of this code is an open question.

In [6] Conway and Sloane have in their table that the highest minimum weight attainable for a length 70 singly-even code is 10 or 12, but this is an error as we shall see. This was also noticed later by Sloane in a private communication. A possible weight enumerator of a singly-even $[70, 35, 14]$ code D has two parameters. It is a simple computation to find the weight enumerators of D and its shadow by Theorem 2.5. This was first computed in [23], however the weight enumerator of the shadow was incorrectly reported. We give the corrected weight enumerators in Tables 2 and 3.

Table 2: The Weight Distribution of a $[70, 35, 14]$ Code

Weight	Frequency
0, 70	1
14, 56	11730
16, 54	150535
18, 52	1345960
20, 50	9393384
22, 48	49991305
24, 46	204312290
26, 44	650311200
28, 42	1627498400
30, 40	3221810284
32, 38	5066556495
34, 36	6348487600

Table 3: The Weight Distribution of the Shadow of a $[70, 35, 14]$ Code

Weight	Frequency
15, 55	87584
19, 51	7367360
23, 47	208659360
27, 43	2119532800
31, 39	8314349120
35	13059745920

Note that any $[70, 35, 14]$ code must have the same weight enumerator as the length 70 child of the extremal doubly-even $[72, 36, 16]$ code. Thus the existence of an extremal doubly-even self-dual code of length 72 is equivalent to the existence of an extremal singly-even self-dual code of length 70. In this section, we generalize this result.

The following lemma is well-known.

Lemma 3.1 *A doubly-even self-dual $[24k, 12k, 4k + 4]$ code is an extremal code and has a unique weight enumerator. Every singly-even $[24k - 2, 12k - 1]$ code is a child of a doubly-even $[24k, 12k]$ code.*

Let C be a doubly-even self-dual $[24k, 12k, 4k + 4]$ code. Corollary 2.8 gives that C has a $[24k - 2, 12k - 1, 4k + 2]$ child, which we denote D . Using Theorem 2.5 we see that there are $\lfloor \frac{n}{8} \rfloor$ unknowns in the weight enumerator after noting that $a_0 = 1$. Since $n = 24k - 2$ we have that $\lfloor \frac{n}{8} \rfloor = 3k - 1$. Requiring that the minimum weight is $4k + 2$ eliminates $2k$ of the unknowns leaving $k - 1$ unknowns.

By Lemma 3.1, we also have that the shadow of D must have minimum weight $4k + 3$. Since there are k weights less than $4k + 3$ congruent to $3 \pmod{4}$, this determines the remaining $k - 1$ unknowns, moreover we have restrictions on the weight enumerator of D . Hence the weight enumerator of D is uniquely determined.

Proposition 3.2 *The weight enumerator of a $[24k - 2, 12k - 1, 4k + 2]$ child of a doubly-even $[24k, 12k, 4k + 4]$ is uniquely determined. The shadow of the child has minimum weight $4k + 3$.*

Remark. By the Assmus-Mattson theorem, vectors of any weight in an extremal doubly-even code of length $24k$ form a 5-design (cf. [2]). Thus, it is possible to show this proposition using properties of a design. This proof was given in [11].

Theorem 3.3 *For fixed k , the existence of a singly-even $[24k - 2, 12k - 1, 4k + 2]$ code whose shadow has minimum weight $4k + 3$ is equivalent to the existence of an extremal doubly-even code of length $24k$.*

Proof. If any singly-even $[24k - 2, 12k - 1, 4k + 2]$ code has a shadow with minimum weight $4k + 3$, then it follows from Theorem 2.6 that the code is a child of an extremal doubly-even $[24k, 12k, 4k + 4]$ code. Thus the existence of two codes is equivalent. \square

Remark. A similar argument can establish the corresponding results for extremal doubly-even codes of length $24k + 8$.

Now we examine the possibilities for weight enumerators of the singly-even $[24k - 2, 12k - 1, 4k + 2]$ codes, showing the details for the case when $k = 4$.

Let us consider the possible weight enumerators of a singly-even $[94, 47, 18]$ code C_{94} . By Theorem 2.5, the possible weight enumerators of C_{94} and its shadow S_{94} are determined. Since the minimum weight of C_{94} is 18, the first equation in Theorem 2.5 gives that

$$\begin{aligned} a_0 &= 1, a_1 = -47, a_2 = 846, a_3 = -7379, a_4 = 32806, \\ a_5 &= -72850, a_6 = 75764, a_7 = -33511, a_8 = 0 \end{aligned}$$

By the second equation in Theorem 2.5, the weight enumerator W_S of S_{94} is

$$-\frac{a_{11}}{524288}y^3 + \left(\frac{a_{10}}{8192} + \frac{11a_{11}}{262144}\right)y^7 + \left(-\frac{a_9}{128} - \frac{5a_{10}}{2048} - \frac{231a_{11}}{524288}\right)y^{11} + \dots$$

Let B_i be the coefficient of y^i in W_S . By Theorem 5 in [6], there exist three possibilities, namely $(B_3, B_7) = (1, 0)$, $(0, 1)$ and $(0, 0)$. It can be easily seen that the first two cases imply a negative or non-integral coefficient. We consider the last case that $B_3 = B_7 = 0$. Since it holds that $a_{10} = a_{11} = 0$,

$$W_S = -\frac{a_9}{128}y^{11} + \frac{9a_9}{64}y^{15} + \dots$$

Since all the coefficients must be non-negative integers, $-\frac{a_9}{128} \geq 0$ and $\frac{9a_9}{64} \geq 0$ then $a_9 = 0$. Thus the minimum weight of the shadow in the last case is 19.

Rains [29] has proven the following:

Theorem 3.4 *The existence of an extremal doubly-even self-dual code of length $24k$ is equivalent to the existence of a singly-even self-dual $[24k - 2, 12k - 1, 4k + 2]$ code.*

The following is immediate.

Corollary 3.5 *Every $[24k - 2, 12k - 1, 4k + 2]$ code is a shadow extremal code.*

Mallows, Odlyzko and Sloane [25] proved that one of the coefficients of the weight enumerators of extremal doubly-even codes is negative for all sufficiently large lengths. Thus there is no singly-even $[24k - 2, 12k - 1, 4k + 2]$ code and singly-even $[24k + 6, 12k + 3, 4k + 2]$ code whose shadow has minimum weight $4k + 3$ for all sufficiently large k . It is mentioned in [25] that A_{d+4} first goes negative when n is about 3270, where A_i is the number of the vectors of weight i in an extremal doubly-even $[n, n/2, d]$ code. It is also shown that $A_{628} < 0$ in an extremal doubly-even $[3720, 1860, 624]$ code. Thus there is no singly-even $[3718, 1859, 622]$ code whose shadow has minimum weight 623.

4 Neighbors of an extremal doubly-even code

In this section, we investigate a neighbor of an extremal doubly-even self-dual code C of length $24k$. Let v be any weight 4 vector of length $24k$. Consider the neighbor $C' = N(C, v)$. That is, if C_0 is the subcode of C with vectors orthogonal to v then $C' = \langle C_0, v \rangle$. Note C' is a doubly-even self-dual code. Also the code C' will have only 1 weight 4 vector and other than this vector, the smallest weight attainable is $4k$. To determine the number of weight $4k$ vectors all that is needed is to know how many of the weight $4k + 4$ vectors meet the 4 non-zero coordinates of v . Since the weight $4k + 4$ vectors hold a 5-design, this number is simply λ_4 for this design, where λ_4 is the number of blocks containing a set of 4 points.

Theorem 4.1 *If C is a doubly-even $[24k, 12k, 4k + 4]$ code, then the neighbor $C' = N(C, v)$ where v is any weight 4 vector, has a uniquely determined weight enumerator.*

Proof. The coefficient of y^4 is 1, the coefficient of y^{4k} is λ_4 , and the coefficient of y^{4s} is 0 for $4 < 4s < 4k$. Since there are only k unknowns, this uniquely determines the weight enumerator. \square

Let E be a $[24k - 4, 12k - 2, 4k]$ child of the code C' as given in Theorem 2.6. That is, if

$$C^* = (0, 0, 0, 0, C_0) \cup (1, 1, 0, 0, C_2) \cup (1, 0, 1, 0, C_1) \cup (0, 1, 1, 0, C_3)$$

then $C' = \langle v, C^* \rangle$.

There are $3k - 1$ unknowns in the possible weight enumerator of E . We note that the minimum weight of the shadow must be at least $4k - 2$. Requiring that the minimum weight of E is $4k$ and that the shadow has minimum weight at least $4k - 2$ leaves 1 unknown. Let c'_{4k} and e_{4k} be the number of weight $4k$ vectors in C' and E , respectively, and s_{4k-2} be the number of weight $4k - 2$ in the shadow. The equation in Theorem 2.6 gives that $c'_{4k} = e_{4k} + 2s_{4k-2}$ determining the last unknown. This gives the following:

Theorem 4.2 *If C' is the weight 4 neighbor of a doubly-even $[24k, 12k, 4k + 4]$ code then the child E of C' is a $[24k - 4, 12k - 2, 4k]$ code and has a uniquely determined weight enumerator.*

To show for a particular k that there is no doubly-even $[24k, 12k, 4k + 4]$ code it is enough to show that the code C' or E as described above does not exist. It is not known if an extremal doubly-even $[24k, 12k, 4k + 4]$ code exists for $k \geq 3$. In particular, a long-standing open question is the existence of an extremal doubly-even $[72, 36, 16]$ code (cf., e.g. [23], [24], [31]). We use this case to give an example.

Let C be an extremal doubly-even $[72, 36, 16]$ code and let v be a weight 4 vector of length 72. Let C' be the neighbor of C which is $N(C, v)$. Then we have that C' is a doubly-even $[72, 36, 4]$ code. The weight enumerator of a possible $[72, 36, 4]$ code has three parameters. Let C'_i denote the number of vectors of weight i in C' . It is clear that $C'_4 = 1$ and $C'_8 = 0$. To find C'_{12} we need to determine how many weight 16 vectors in C meet the 4 coordinates of v . The weight 16 vectors in C form a 5-design with $\lambda_4 = 442$, hence $C'_{12} = 442$. Hence the weight enumerator of C' is determined as well as the weight enumerator of C_0 , where the results are given in Table 4.

Let E be a $[24k - 4, 12k - 2, 4k]$ child of the code C' as given in Theorem 2.6. That is, if

$$C^* = (0, 0, 0, 0, C_0) \cup (1, 1, 0, 0, C_2) \cup (1, 0, 1, 0, C_1) \cup (0, 1, 1, 0, C_3)$$

then $C' = \langle v, C^* \rangle$.

Table 4: The Weight Distribution of the Weight 4 Neighbor and its Subcode

Weight	C_0	C'
	Frequency	Frequency
0, 72	1	1
4, 68	0	1
12, 60	0	442
16, 56	134521	264673
20, 52	9284176	18589296
24, 48	232444043	464824659
28, 44	2196187840	4392509606
32, 40	8298695163	16597183691
36	12886246880	25772731998

There are 8 unknowns in the possible weight enumerator of E . Requiring that the minimum weight of E is 12 and that the shadow has minimum weight at least 10 leaves 1 unknown. Let c'_{12} and e_{12} be the number of weight 12 vectors in C' and E , respectively, and s_{10} be the number of weight 10 in the shadow. As described before we have $c'_{12} = e_{12} + 2s_{10}$ determining the last unknown. Thus we can determine the weight distribution where the results are listed in Table 5.

Table 5: The Weight Distribution of the Child of the Weight 4 Neighbor

Weight	Frequency
0, 68	1
12, 56	442
14, 54	14960
16, 52	174471
18, 50	1478048
20, 48	9546537
22, 46	46699952
24, 44	175078410
26, 42	509477760
28, 40	1160564636
30, 38	2081169376
32, 36	2949602799
34	3312254400

Now we give necessary conditions based on the neighbors for the existence of an extremal doubly-even code of length 72. By Theorem 4.2, the weight enumerator of the $[72, 36, 4]$ neighbor of an extremal doubly-even $[72, 36, 16]$ code is uniquely determined. We consider self-dual codes of length 70 which can be extended to the $[72, 36, 4]$ neighbor N . It follows from Corollary 2.8 that N is a parent of a self-dual $[70, 35]$ code D with

$$N = (0, 0, D_0) \cup (1, 1, D_2) \cup (1, 0, D_1) \cup (0, 1, D_3)$$

where D_0 is the subcode of doubly-even vectors of D . By the weight enumerator of N , D has the following properties:

- (1) There is no weights 6 and 8 vector in D ,
- (2) The minimum weight of D is less than or equal to 12,
- (3) There is no weight 7 vector in S and
- (4) There is a weight 2 or 4 vector in D if and only if there is no weight 3 vector in S .

where S is the shadow of D . By Theorems 2.5 and 2.6, the possible weight enumerators of D are determined. The result is listed in Table 6, where d denotes the minimum weight of D .

Theorem 4.3 *If no self-dual $[70, 35, d]$ code with weight enumerator given in Table 6 exists, then there exists no extremal doubly-even $[72, 36, 16]$ code.*

Proof. If no self-dual $[70, 35, d]$ code with weight enumerator given in Table 6 exists, then the $[72, 36, 4]$ neighbor does not exist. Thus there exists no extremal doubly-even code of length 72. \square

Table 6: The Possible Weight Enumerators of D

	$d = 2$	$d = 4$	$d = 10$	$d = 12$
a_0	1	1	1	1
a_1	-34	-35	-35	-35
a_2	391	421	420	420
a_3	-1802	-2088	-2065	-2065
a_4	3179	4146	4025	4025
a_5	-1870	$-2988 \leq a_5 \leq -2910$	$-2737 \leq a_5 \leq -2698$	-2737
a_6	0	$-4a_5 - 11640$	$-4a_5 - 10584$	364
a_7	0	0	-2048	-2048
a_8	0	0	8192	8192

5 Extremal singly-even $[68, 34, 12]$ codes

Applying Theorem 2.5 to a putative self-dual $[68, 34, 14]$ code and examining the weight enumerator of the shadow shows that there is no possible self-dual code for these parameters. Applying the same to a possible $[68, 34, 12]$ code, the possibilities for the weight enumerators of such a code and its shadow are determined. The weight enumerators are given in Tables 7 and 8.

Table 7: Possible Weight Enumerators for [68, 34, 12] Codes

the coefficient of y^i	weight i
1	0
$442 + a_6$	12, 56
$14960 - 2a_6 + a_7$	14, 54
$-9a_6 + a_8 + 174471 - 8a_7$	16, 52
$1478048 - 14a_8 + 20a_6 + 22a_7$	18, 50
$35a_6 + 89a_8 - 8a_7 + 9546537$	20, 48
$-90a_6 - 336a_8 - 83a_7 + 46699952$	22, 46
$820a_8 + 160a_7 - 75a_6 + 175078410$	24, 44
$8a_7 + 509477760 + 240a_6 - 1288a_8$	26, 42
$-352a_7 + 90a_6 + 1092a_8 + 1160564636$	28, 40
$338a_7 - 420a_6 + 2081169376 + 208a_8$	30, 38
$-42a_6 - 2002a_8 + 208a_7 + 2949602799$	32, 36
$3312254400 + 504a_6 - 572a_7 + 2860a_8$	34

Table 8: Possible Weight Enumerators for the Shadows of [68, 34, 12] Codes

the coefficient of y^i	weight i
$\frac{1}{16384}a_8$	2, 66
$\frac{-1}{256}a_7 - \frac{1}{1024}a_8$	6, 62
$\frac{7}{128}a_7 + \frac{15}{2048}a_8 + \frac{1}{4}a_6$	10, 58
$\frac{-91}{256}a_7 - \frac{35}{1024}a_8 + 29920 - 3a_6$	14, 54
$\frac{33}{2}a_6 + \frac{455}{4096}a_8 + 2956096 + \frac{91}{64}a_7$	18, 50
$-55a_6 + 93399904 - \frac{273}{1024}a_8 - \frac{1001}{256}a_7$	22, 46
$\frac{1001}{2048}a_8 + 1018955520 + \frac{1001}{128}a_7 + \frac{495}{4}a_6$	26, 40
$\frac{-3003}{256}a_7 + 4162338752 - 198a_6 - \frac{715}{1024}a_8$	30, 38
$\frac{429}{32}a_7 + 231a_6 + \frac{6435}{8192}a_8 + 6624508800$	34

It follows from Theorem 4.2 that the weight enumerator of the child of the neighbor of an extremal doubly-even [72, 36, 16] code is uniquely determined. The child is a shadow extremal singly-even [68, 34, 12] code with weight enumerator determined by $a_6 = a_7 = a_8 = 0$. Thus we are interested in the weight enumerators for which there are extremal singly-even [68, 34, 12] codes.

6 Automorphism Group

The automorphism group of a code C denoted by $Aut(C)$ is the set of all permutations of the coordinates that preserves the code.

The number of codes that are equivalent to a binary code C is $\frac{n!}{|Aut(C)|}$. If a Type II [72, 36, 16] code exists then there are two possible explanation as to why it is difficult to find. First is that $|Aut(C)|$ is very large and hence there are very few codes equivalent to the code to find. The second is that $|Aut(C)|$ is very small and even though there are many equivalent copies of the code it remains hard to find because its structure is not interesting.

Several results about the automorphism group are known. In [5], it was shown 23 is the largest odd prime dividing the order of the automorphism group of this code. In [28], it was shown that 23 also does not divide the order and 11 was eliminated in [22]. Hence the only possible primes dividing the order of the automorphism group of a putative [72, 36, 16] Type II code are 2, 3, 5 and 7. In [3], it was shown that any automorphism of order 2 cannot have any fixed points.

7 Designs

Another important aspect of these codes are the designs formed from the vectors of a given weight. We shall give the basic definitions and state the most important theorem in this connection. For a complete description of codes and designs we suggest Assmus and Key [1].

Definition 7.1 *An incidence structure $D = (P, B, I)$ is a $t - (v, k, \lambda)$ design, where t, v, k, λ are non-negative integers, if*

- $|P| = v$;
- every block $b \in B$ is incident with precisely k points;
- every t distinct points are together incident with precisely λ blocks.

Numerous arithmetic conditions hold for these parameters, see Chapter 1 of [1]. In addition there are the parameters λ_s which are the number of blocks incident with s distinct points. A standard technique in showing the non-existence of a design is showing that at least one of the parameters is not a non-negative integer.

The principle theorem in the connection between codes and designs is the Assmus-Mattson Theorem first proven in by Assmus and Mattson, it can be found in [1]. We shall state it only in its form for binary codes, although the general version is for codes over any finite field.

Theorem 7.2 (Assmus-Mattson) *Let C be a binary code of block length n with minimum weight d , and let d^\perp denote the minimum weight of C^\perp . Suppose there is an integer t with $0 < t < d$ that satisfies the following condition: for $W_C^\perp(1, y) = \sum B_i y^i$ at most $d - t$ of B_1, B_2, \dots, B_{n-t} are non-zero. Then for each i with $d \leq i \leq n$ the supports of the vectors of weight i of C , provided there are any, yield a t -design. Similarly, for j with $d^\perp \leq j \leq n - t$ the supports of the vectors of weight j in C^\perp , provided there are any, form a t -design.*

If this theorem is applied to the [72, 36, 16] code then it is well known that each of the weights form 5-designs.

Let D be a $[70, 35, 14]$ Type I code, and let D_0 be the subcode of doubly-even vectors. The weight enumerators for D_0 and D_0^\perp can be easily calculated using Tables 2 and 3. It follows from the Assmus-Mattson Theorem that the vectors of any weight in D_0 and D_0^\perp hold 3-designs. This gives divisibility conditions on the coefficients of the shadow if a code exists, namely the λ_j for $j = 1, 2, 3$ for each weight must be integers. The following table gives those values.

Table 9: Design Parameters

i	λ_1	λ_2	λ_3
15	18768	3808	728
19	1999712	521664	130416
23	68559504	21859552	6750744
27	817534080	308056320	113256000
31	3682068896	1600899520	682736560
35	6529872960	3217618560	1561491360
39	4632280224	2551110848	1388104432
43	1301998720	792520960	477843520
47	140099856	93399904	61808760
51	5367648	3889600	2802800
55	68816	53856	41976

Table 10: The weight enumerator of the weight 4 neighbor and its subcode

C_{0_i}	C'_i	i
1	1	0
0	1	4
0	442	12
134521	264673	16
9284176	18589296	20
232444043	464824659	24
2196187840	4392509606	28
8298695163	16597183691	32
12886246880	25772731998	36

8 Higher Weights

We shall give the definition of higher weights, introduced by Wei [33], following the notation in [32]. Let $D \subseteq \mathbb{F}_2^n$ be a linear subspace, then

$$(9) \quad ||D|| = |Supp(D)|,$$

where

$$(10) \quad Supp(D) = \{i \mid \exists v \in D, v_i \neq 0\}.$$

Table 11: The weight enumerator of the child of the weight 4 neighbor

E_i	i
1	0
442	12
14960	14
174471	16
1478048	18
9546537	20
46699952	22
175078410	24
509477760	26
1160564636	28
2081169376	30
2949602799	32
3312254400	34

For a linear code C define

$$(11) \quad d_r(C) = \min\{\|D\| \mid D \subseteq C, \dim(D) = r\}.$$

The higher weight spectrum is defined as

$$(12) \quad A_i^r = |\{D \subseteq C \mid \dim(D) = r, \|D\| = i\}|.$$

and then we define the higher weight enumerator by

$$(13) \quad W^r(C; y) = W^r(C) = \sum A_i^r y^i.$$

In [9] a Gleason's theorem for higher weight enumerators is given and the second higher weight enumerator for the putative length 72 code is given and follows in Table 12.

9 Codes from Designs

We examine designs with the parameters of a design formed from the codewords of an extremal Type II code. We show that the vectors of any non-trivial weight other than 28 and 44 generate the $[72, 36, 16]$ Type II code and that the vectors of any non-trivial weight other than 48 generate the $[96, 48, 20]$ Type II code.

In this work we examine these code via the designs formed from their vectors of a given work. The Assmus-Mattson theorem gives that the vectors of non-trivial weight form a 5-design for any $[24k, 12k, 4k + 4]$ code and we examine the code formed from these designs. We begin with some definitions.

For a $t - (v, k, \lambda)$ design every subset of size i , $i \leq t$, is contained in λ_i vectors. These values follow from the computation

$$\lambda_i = \lambda \binom{v-i}{t-i} / \binom{k-i}{t-i}.$$

Table 12: The Second Higher Weight Enumerator for a Type II $[72, 36, 16]$ Code

coefficient of y^i	weight i
96191865	24
4309395552	26
119312891460	28
2379079500864	30
37327599503964	32
466987648992480	34
4687779244903412	36
37810235197002240	38
244777798274765679	40
1269000323938260672	42
5251816390965277320	44
17262594429823645056	46
44763003632389491540	48
90768836016453484224	50
142313871132195291144	52
170060449665123790080	54
152060783100409784007	56
99349931253373567200	58
45970401654169517364	60
14440224673488398400	62
2900924791551272475	64
340809968304405600	66
20197782231604740	68
451381581930240	70
1617151596337	72

The characteristic function of a block is $\chi_v(q) = 1$ if and only if the point q is incident with the block v . For a design D we define $C_p(D)$ to be the code over \mathbb{F}_p defined by $C_p(D) = \langle \chi_v \mid v \text{ a block in } D \rangle$. In this work we only consider $p = 2$. A self-orthogonal design is a design where the parity of the vectors is the same as the parity of the intersection numbers of blocks.

Let C be a Type II, $[24\alpha, 12\alpha, 4\alpha + 4]$ extremal code. The Assmus-Mattson theorem [2] gives that the vectors of any weights form a 5-design.

Lemma 9.1 *Let D be a self-orthogonal design with the parameters of a design formed by the Assmus-Mattson theorem applied to a Type II, $[24\alpha, 12\alpha, 4\alpha + 4]$ extremal code. Then $C_2(D)$ is a doubly-even self-orthogonal code.*

Proof. The characteristic functions of blocks have weight congruent to 0 (mod 4) and the intersection numbers are even so the generating vectors are all orthogonal. \square

Let D be a $t - (v, k, \lambda)$ design, then the complimentary design, D^c , formed by the complements of blocks is a $t - (v, v - k, b - 2r - \lambda)$ design where b is the number of blocks and r is the number of blocks through a point.

Theorem 9.2 *Let D be a self-orthogonal design with the parameters of a design formed by the Assmus-Mattson theorem applied to a Type II, $[24\alpha, 12\alpha, 4\alpha + 4]$ extremal code. If $C_2(D)^\perp$ and $C_2(D^c)^\perp$ are even codes then $C_2(D) = C_2(D^c)$.*

Proof. We know that $\langle C_2(D), \mathbf{1} \rangle = C_2(D^c)$ and $\langle C_2(D^c), \mathbf{1} \rangle = C_2(D)$. If C^\perp is even then $\mathbf{1}$ is in C and so then the two codes must be equal. \square

This theorem will be very useful to us since the code of every design we consider in this work will have this property. Hence we will only have to consider the design with parameters for half of the possible weights.

The following is given for specific designs in [20] and [17].

Theorem 9.3 *Let D be a 5-design with the parameters of a design formed from the Assmus-Mattson theorem applied to a Type II $[24\alpha, 12\alpha, 4\alpha + 4]$ extremal code. Let $w \in C_2(D)^\perp$ of weight m and let n_i be the number of blocks intersecting $\text{Supp}(w)$ in i positions. Then we have*

$$(14) \quad \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{2i}{j} n_{2i} = \lambda_j \binom{m}{j},$$

for $j = 0, 1, \dots, 5$.

Proof. There are $\binom{m}{j}$ different sets of j coordinates in the support of w and λ_j blocks through each of these j points. We can count the same by noticing that each block that intersects w in $2i$ places can intersect it in one of $\binom{2i}{j}$ sets of j coordinates and there are n_{2i} such blocks. \square

The following two lemmas refer to the values in the set of equations. The first lemma is evident.

Lemma 9.4 *If $2i > k$, where k is the block size, then $n_{2i} = 0$.*

Lemma 9.5 *Let D be a design and $w \in C_2(D)^\perp$ of weight m . Let n_{2i} be the number of blocks of D that intersects $\text{Supp}(w)$ in exactly $2i$ places and let n'_{2i} be the number of blocks of D that intersects the complement of $\text{Supp}(w)$ in exactly $2i$ places. Then $n_{2i} = n'_{k-2i}$.*

Proof. If w is a vector of weight m then its complement is a vector of weight $v - m$. If a block of size k intersects $\text{Supp}(w)$ in exactly $2i$ positions then it intersects its complement in exactly $k - 2i$ places, therefore $n_{2i} = n'_{k-2i}$. \square

This lemma relates the computation of the number of weight m vectors in the orthogonal with the number of weight $v - m$ vectors in the orthogonal. Specifically, when we compute n_{2i} for weight m vectors in the orthogonal we have n_{2i} is equal to the value of n_{k-2i} when computing weight $v - m$ vectors. Since the all one-vector is the orthogonal of the code of the design for self-orthogonal designs with the parameters of the design formed the extremal codes, then if there are vectors of weight m then there are an equal number of weight $v - m$ vectors.

Lemma 9.6 *Let m and n_{2i} be as defined before. If $4m + k - 2i > v$ then $n_{2i} = 0$.*

Proof. If $n_{2i} \neq 0$ then the vector resulting from the sum of the vector of weight m and the block of weight k intersecting it in $2i$ places has support size greater than v , which is the length of the code. \square

Lemma 9.7 *If C is a doubly-even code then it is self-orthogonal. A code that is doubly-even and has a doubly-even orthogonal must be self-dual.*

Proof. If $v, w \in C$ then $wt(v + w) = wt(v) + wt(w) - 2|v \wedge w|$. Since all of the weights are $0 \pmod{4}$ then $|v \wedge w|$ must be even and the code must be self-orthogonal. If C and C^\perp are both doubly even then $C \subset C^\perp$ and $C^\perp \subset C$ so $C = C^\perp$. \square

The following computational approach is taken. Using the system of equations given in equation 14 for a specific design we determine if there are solutions for each m with $1 \leq m \leq n$, where n is the length of the code. If there are no solutions when $m \not\equiv 0 \pmod{4}$ then the dual must be doubly-even and so the code of the design must be self-dual. Additionally, we can determine what the possible minimum weight can be by examining the smallest m that has solutions to the system of equations. Finally we apply Lemma 9.4, Lemma 9.5 and Lemma 9.6 and eliminate n_{2i} .

Additionally, we use the following.

Lemma 9.8 *If C is a Type II extremal code and the vectors form a design whose code is self-dual then it is equal to C .*

Proof. The lemma is immediate noting that $C_2(D) \subseteq C$. \square

This is different than simply considering an arbitrary design since we are assuming that the code exists, whereas it is possible for some of the designs to exist without the code existing. It is well known the vectors of weight 8, 12 and 16 generate the binary Golay $[24, 12, 8]$ code so we begin with the next case.

9.1 The $[48, 24, 12]$ Extremal Type II Code

The weight enumerator of an extremal Type II code of length 48 is:

$$1 + 17296y^{12} + 535095y^{16} + 3995376y^{20} + 7681680y^{24} \\ + 3995376y^{28} + 535095y^{32} + 17296y^{36} + y^{48}.$$

- The weight 12 vectors form a $5 - (48, 12, 8)$ design with 17296 blocks. Given an arbitrary design D with these parameters we have: $C_2(D)$ is a $[48, 24, 12]$ Type II code.
- The weight 16 vectors form a $5 - (48, 16, 1365)$ design with 535095 blocks. Given an arbitrary design D with these parameters we have: $C_2(D)$ is a $[48, 24, 12]$ Type II code.
- The weight 20 vectors form a $5 - (48, 20, 36176)$ design with 3995376 blocks. Given an arbitrary design D with these parameters we have: $C_2(D)$ is a $[48, 24, 12]$ Type II code.
- The weight 24 vectors form a $5 - (48, 24, 190680)$ design with 7681680 blocks. Given an arbitrary design D with these parameters we have: Solving the equations in equation 14 we have a unique solution, namely $n_0 = 27240$, $n_2 = 1525440$, $n_4 = 4576320$, $n_6 = 1525440$, $n_8 = 27240$. This do not give a contradiction. Therefore, $C_2(D)$ is a $[48, 24, \geq 8]$ Type II code.

Applying Lemma 9.8 to these results we get the following.

Theorem 9.9 *Let C be a $[48, 24, 12]$ Type II code. Then the vectors of any weight other than 0 and 48 generate the code C .*

Summarizing the results we have the following:

Theorem 9.10 *Let D be a self-orthogonal design with the parameters the same as those for the blocks of any weights except 24 as given by the Assmus-Mattson theorem formed from a $[48, 24, 12]$ code has $C_2(D)$ is an extremal $[48, 24, 12]$ Type II code.*

9.2 The $[72, 36, 16]$ Extremal Type II Code

The weight enumerator of an extremal Type II code of length 72 is:

$$1 + 249849y^{16} + 18106704y^{20} + 462962955y^{24} + 4397342400y^{28} \\ + 16602715899y^{32} + 25756721120y^{36} + 16602715899y^{40} + 4397342400y^{44} \\ + 462962955y^{48} + 18106704y^{52} + 249849y^{56} + y^{72}$$

- It is shown in [20] that the designs with the parameters of the weight 16 vectors generate a $[72, 36, 16]$ Type II code.
- The weight 20 vectors form a $5 - (72, 20, 20064)$ design with 18106704 blocks. Given an arbitrary design D with these parameters we have: Applying the standard lemma and noticing that n_{12} must be 0 since otherwise there would be a weight 8 vector, which we know there is not, there is a unique solution for $m = 12$ that is $n_0 = 484440$, $n_2 = 7101930$, $n_4 = 8553600$, $n_6 = 1902780$, $n_8 = 59400$, $n_{10} = 4554$. No contradiction is reached from this values. Therefore, $C_2(D)$ is a $[72, 36, \geq 12]$ Type II code.
- The weight 24 vectors form a $5 - (72, 24, 1406405)$ design with 462962955 blocks. Given an arbitrary design D with these parameters we have:
 $C_2(D)$ is a $[72, 36, \geq 12]$ Type II code.
- The weight 28 vectors form a $5 - (72, 28, 30888000)$ design with 4397342400 blocks. Given an arbitrary design D with these parameters we have:
 $C_2(D)$ is a length 72 self-orthogonal code with minimum distance at least 12. Solving the system of equations formed in Equation 14 for $m = 10$ there are solution with 1 unknown. However there are no substitutions for the unknown that makes all $n_{2i} \geq 0$. Hence there are no vectors of weight 10.
- The weight 32 vectors form a $5 - (72, 32, 238957796)$ design with 16602715899 blocks. Given an arbitrary design D with these parameters we have:
 $C_2(D)$ is a $[72, 36, \geq 12]$ Type II code.
- The weight 36 vectors form a $5 - (72, 36, 693996160)$ design with 25756721120 blocks. Given an arbitrary design D with these parameters we have:
 $C_2(D)$ is a $[72, 36, \geq 12]$ Type II code.

Applying Lemma 9.8 to these results we get the following.

Theorem 9.11 *Let C be a $[72, 36, 16]$ Type II code. Then the vectors of any weight other than 0, 28, 44, and 72 generate the code C .*

9.3 The $[96, 48, 20]$ Extremal Type II Code

The weight enumerator of an extremal Type II code of length 96 is:

$$\begin{aligned}
& 1 + 3217056 y^{20} + 369844880 y^{24} + 18642839520 y^{28} + 422069980215 y^{32} \\
& + 4552866656416 y^{36} + 24292689565680 y^{40} + 65727011639520 y^{44} + 91447669224080 y^{48} \\
& + 65727011639520 y^{52} + 24292689565680 y^{56} + 4552866656416 y^{60} + 422069980215 y^{64} \\
& + 18642839520 y^{68} + 369844880 y^{72} + 3217056 y^{76} + y^{96}
\end{aligned}$$

- It is shown in [17] that the designs with the parameters of the weight 20 vectors generate a $[96, 48, 20]$ Type II code.
 - The weight 24 vectors form a $5 - (96, 24, 257180)$ design with 369844880 blocks. Given an arbitrary design D with these parameters we have:
 $C_2(D)$ is a $[96, 48, \geq 16]$ Type II code.
 - The weight 28 vectors form a $5 - (96, 28, 29975400)$ design with 18642839520 blocks. Given an arbitrary design D with these parameters we have:
 $C_2(D)$ is a $[96, 48, \geq 12]$ Type II code.
 - The weight 32 vectors form a $5 - (96, 32, 1390528685)$ design with 422069980215 blocks. Given an arbitrary design D with these parameters we have:
 $C_2(D)$ is a $[96, 48, \geq 12]$ Type II code.
 - The weight 36 vectors form a $5 - (96, 36, 28080500448)$ design with 422069980215 blocks. Given an arbitrary design D with these parameters we have:
 $C_2(D)$ is a $[96, 48, \geq 12]$ Type II code.
 - The weight 40 vectors form a $5 - (96, 40, 261513764460)$ design with 24292689565680 blocks. Given an arbitrary design D with these parameters we have:
 $C_2(D)$ is a $[96, 48, \geq 12]$ Type II code.
 - The weight 44 vectors form a $5 - (96, 44, 1167789832440)$ design with 65727011639520 blocks. Given an arbitrary design D with these parameters we have:
 $C_2(D)$ is a $[96, 48, \geq 12]$ Type II code.
 - The weight 48 vectors form a $5 - (96, 48, 2561776811880)$ design with 91447669224080 blocks. Given an arbitrary design D with these parameters we have:
 $C_2(D)$ is a self-orthogonal code with minimum distance at least 8.
- Applying Lemma 9.8 to these results we get the following.

Theorem 9.12 *Let C be a $[96, 48, 20]$ Type II code. Then the vectors of any weight other than 0, 48 and 96 generate the code C .*

For this code the only arbitrary design that we can be sure generates the code (without the assumption that the code exists, is the design of minimum weight vectors and its complimentary design.

10 Open Problems

- Prove that the $[70, 35, 14]$ Type I code with weight enumerator given above does not exist or construct it and then the length 72 code from it.
- Prove that the $[68, 34, 12]$ Type I code with weight enumerator given above does not exist or construct it and then the length 72 code from it.
- Show that one of the designs given in the paper does not exist showing that the code does not exist.
- Find one of the designs given in the paper and examine the code generated by the incidence vectors of the blocks and determine if they construct one of the codes.
- Compute the third (or higher) weight enumerator for the length 72 code in hope of finding a coefficient that is not a non-negative integer.

References

- [1] E.F. Assmus, Jr. and J.D. Key, *Designs and Their Codes*, Cambridge University Press.
- [2] E.F. Assmus, Jr., and H.F. Mattson, Jr., New 5-designs, *J. Combin. Theory* vol. 6, pp. 122–151, 1969.
- [3] Bouyuklieva, S., On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length $24m$, preprint.
- [4] R.A. Brualdi and V.S. Pless, Weight enumerators of self-dual codes, *IEEE Trans. Inform. Theory* vol. IT-37, pp. 1222–1225, 1991.
- [5] J.H. Conway and V. Pless, On primes dividing the group order of a doubly $(72, 36, 16)$ code and the group order of a quaternary $(24, 12, 10)$ code, *Discrete Math.*, Vol. 38, 143-156, 1982.
- [6] 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. IT-36, pp. 1319–1333, 1990.
- [7] S.T. Dougherty, Shadow codes and weight enumerators, *IEEE Trans. Inform. Theory* vol. IT-41, pp. 762–768, 1995.
- [8] S.T. Dougherty, An Elusive Doubly-Even Binary Self-Dual Code, preprint, 1994.
- [9] Steven T. Dougherty and T. Aaron Gulliver, Higher Weights and Binary Self-Dual Codes , *WCC 2001*, 177-188, 2001.

- [10] S.T. Dougherty, T.A. Gulliver, and M. Harada, Extremal Binary Self-Dual Codes *IEEE Trans. Inform. Theory*, Vol. 43, No. 6, 1997.
- [11] S.T. Dougherty and M. Harada, Shadow Optimal Self-Dual Codes, *Kyushu Journal of Mathematics*, Vol 53, No. 2., 1999, p. 223-237.
- [12] W. Feit, A self-dual even $(96, 48, 16)$ code, *IEEE Trans. Inform. Theory* vol. IT-20, pp. 136–138, 1974.
- [13] A.M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, *Actes Congres Internl. de Mathematique*, Vol. 3, 211-215, 1970.
- [14] T.A. Gulliver and M. Harada, Classification of extremal double circulant self-dual codes of lengths 64 to 72, (submitted).
- [15] M. Hall, Jr., *Combinatorial Theory (2nd ed.)*. New York: Wiley, 1986.
- [16] M. Harada, The existence of a self-dual $[70, 35, 12]$ code and formally self-dual codes, (submitted).
- [17] M. Harada, *Remark on a 5-design related to a putative extremal doubly-even self-dual $[96, 48, 20]$ code*, to appear.
- [18] M. Harada, T.A. Gulliver and H. Kaneta, Classification of extremal double circulant self-dual codes of length up to 62, (submitted).
- [19] M. Harada and H. Kimura, New extremal doubly-even $[64, 32, 12]$ codes, *Des. Codes and Cryptogr.* vol. 6, pp. 91–96, 1995.
- [20] M. Harada, M. Kitazume and A. Munemasa, *On a 5-design related to an extremal doubly even self-dual code of length 72*, *J. Combin. Theory Ser. A*, **107**, (2004), 143-146.
- [21] W.C. Huffman and V.S. Pless, *Fundamentals of Error-correcting Codes*, Cambridge: Cambridge University Press, 2003.
- [22] Huffman, W.C. and Yorgov, V.Y., A $[72, 36, 16]$ doubly even code does not have an automorphism of order 11, *IEEE Trans. Inform. Theory*, Vol. 33, No. 5, 749-752, 1987.
- [23] G.T. Kennedy and V. Pless, A coding theoretic approach to extending designs, *Discrete Math.* vol. 142, pp. 155–168, 1995.
- [24] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

- [25] C.L. Mallows, A.M. Odlyzko and N.J.A. Sloane, Upper bounds for modular forms, lattices, and codes, *J. Algebra* vol. 36, pp. 68–76, 1975.
- [26] C.L. Mallows and N.J.A. Sloane, *An upper bound for self-dual codes*, Inform. Control **22**, (1973), 188-200.
- [27] V. Pless, Parents, Children, Neighbors and the Shadow, *Contemporary Mathematics*, Vol. 168, 279-290, 1994.
- [28] V. Pless and J.G. Thompson, 17 does not divide the order of the group of a $(72, 36, 16)$ doubly even code, *IEEE Trans. Inform. Theory* Vol. 28, No. 3, 537 - 541, 1982.
- [29] E. Rains, Shadow Bounds of Self-Dual Codes.
- [30] E.Rains and N.J.A. Sloane, *Self-dual Codes*, in the Handbook of Coding Theory, V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, 1998, 177-294.
- [31] N.J.A. Sloane, Is there a $(72, 36)$ $d = 16$ self-dual code?, *IEEE Trans. Inform. Theory* vol. IT-19, p. 251, 1973.
- [32] Michael A. Tsfasman and Serge G. Vladut, Geometric approach to higher weights, *IEEE Trans. Inform. Theory* Vol. 41, 1564–1588, 1995.
- [33] V.K. Wei, Generalized hamming weights for linear codes, *IEEE Trans. Inform. Theory*, Vol. 37, 1412-1418, 1991.