On the existence of certain optimal self-dual codes with lengths between 74 and 116

Tao Zhang* Jerod Michel† Tao Feng‡ Gennian Ge§¶

Submitted: Apr 26, 2015; Accepted: Nov 17, 2015; Published: Nov 27, 2015
Mathematics Subject Classifications: 94B05, 11T71

Abstract

The existence of optimal binary self-dual codes is a long-standing research problem. In this paper, we present some results concerning the decomposition of binary self-dual codes with a dihedral automorphism group D_{2p}, where p is a prime. These results are applied to construct new self-dual codes with length 78 or 116. We obtain 16 inequivalent self-dual $[78, 39, 14]$ codes, four of which have new weight enumerators. We also show that there are at least 141 inequivalent self-dual $[116, 58, 18]$ codes, most of which are new up to equivalence. Meanwhile, we give some restrictions on the weight enumerators of singly even self-dual codes. We use these restrictions to exclude some possible weight enumerators of self-dual codes with lengths 74, 76, 82, 98 and 100.

Keywords: self-dual code, automorphism, weight enumerator

1 Introduction

Binary self-dual codes have been of particular interest for some time now. The extended Hamming $[8, 4, 4]$ code, the extended Golay $[24, 12, 8]$ code and certain extended quadratic

*School of Mathematical Sciences, Capital Normal University, Beijing, China; School of Mathematical Sciences, Zhejiang University, Hangzhou, Zhejiang, China. zhant220@163.com

†School of Mathematical Sciences, Zhejiang University, Hangzhou, Zhejiang, China. samarkand_city@126.com

‡School of Mathematical Sciences, Zhejiang University, Hangzhou, Zhejiang, China; Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing, China. tfeng@zju.edu.cn

§School of Mathematical Sciences, Capital Normal University, Beijing, China; Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing, China. gnge@zju.edu.cn

¶The research of T. Feng was supported by Fundamental Research Fund for the Central Universities of China, the National Natural Science Foundation of China under Grant No. 11201418 and Grant No. 11422112.The research of G. Ge was supported by the National Natural Science Foundation of China under Grant Nos. 61171198, 11431003 and 61571310, and the Importation and Development of High-Caliber Talents Project of Beijing Municipal Institutions.

residue codes are well-known examples of binary self-dual codes. It is known [31] that if there is a natural number $r > 1$ that divides the weight of all vectors in a binary self-dual code C, then $r = 2$ or 4. A binary self-dual code in which all weights are divisible by 4 is called a doubly even self-dual (or Type II) code, otherwise we call it a singly even self-dual (or Type I) code. All doubly even self-dual codes of length up to 40 have been classified [34], [35], [13], [2] and a classification of singly even self-dual codes of length up to 38 is also known [34], [35], [13], [4], [3], [28], [6].

Let C be a binary self-dual code of length n and minimum distance d. By results of Mallows-Sloane [33] and Rains [36], we have

$$d \leqslant \begin{cases} 4\lfloor \frac{n}{24} \rfloor + 4; & \text{if } n \not\equiv 22 \pmod{24}, \\ 4\lfloor \frac{n}{24} \rfloor + 6; & \text{if } n \equiv 22 \pmod{24}. \end{cases}$$

The code C is called extremal if the above equality holds. If $d = 4\lfloor \frac{n}{24} \rfloor + 2$ and $n \not\equiv 22 \pmod{24}$ or if $d = 4\lfloor \frac{n}{24} \rfloor + 4$ and $n \equiv 22 \pmod{24}$ then we say C is near extremal. If there is no extremal code with a given length, then we are interested in the code that attains the largest possible minimum distance. Such a code is called an optimal code. A list of possible weight enumerators of extremal self-dual codes of length up to 72 was given by Conway and Sloane in [14]. This list was extended by Dougherty, Gulliver, and Harada in [18], where lengths are listed up to 100. However, the existence of some extremal self-dual codes is still unknown. For the classification and enumeration of binary self-dual codes, a survey of known results can be found in [30], [37]. For the database of self-dual codes, we refer the reader to [26], [19].

For self-dual codes with large length, a complete classification seems to be impossible. Researchers have focused on self-dual codes with the largest possible minimum weights. Many methods have been proposed to find new self-dual codes with good parameters. Searching for such codes with a double circulant form is a very efficient way, which has led to many good codes [21], [22], [25]. Harada [24] developed a method involving the double extension of codes. Gaborit and Otmani [20] gave a general experimental method to construct self-dual codes. Huffman [29] constructed binary self-dual codes by applying the automorphism of codes.

In recent years there have been extensive efforts on the construction of self-dual codes by prescribing certain automorphisms. In 1982, Huffman [29] investigated binary self-dual codes with automorphisms of odd prime order and derived the decomposition of such a code as a direct sum of two subcodes. In 1983, Yorgov [43] improved this method and derived necessary and sufficient conditions for codes to be equivalent. In 1997, Buyuklieva [12] developed a new method for constructing binary self-dual codes having an automorphism of order 2. In 2004, Dontcheva et al. [17] extended the results to the decomposition of binary self-dual codes possessing an automorphism of order pq, where p and q are odd prime numbers. This technique yields many extremal or optimal codes which possess an automorphism (see [9], [10], [11], [15], [39], [41], [40], [42]).

Let C be a singly even self-dual $[n, n/2, d]$ code and let C_0 be its doubly even subcode that contains all the codewords of weight divisible by 4. There are three cosets C_1, C_2, C_3 of C_0 such that $C_0^{\perp} = C_0 \bigcup C_1 \bigcup C_2 \bigcup C_3$ and $C = C_0 \bigcup C_2$. The set $S = C_1 \bigcup C_3$ is called the shadow of C. Concerning the weight enumerator for S, the following theorem was given in [14].

Theorem 1. *Let $S(y) = \Sigma_{r=0}^{n} B_r y^r$ be the weight enumerator of S. Then the following hold:*

1. $B_r = B_{n-r}$ *for all* r,
2. $B_r = 0$ *unless* $r \equiv n/2 \pmod 4$,
3. $B_0 = 0$,
4. $B_r \leqslant 1$ *for* $r < 2n/d$,
5. *at most one of* B_r *is nonzero for* $r < (d+4)/2$.

It was shown in [18], [27], [22] that the weight enumerator of a binary self-dual $[78, 39, 14]$ code and its shadow weight enumerator have one of the forms

$$W_{78,1} = 1 + (3705 + 8\beta)y^{14} + (62244 + 512\alpha - 24\beta)y^{16} + (774592 - 4608\alpha - 64\beta)y^{18} + \cdots,$$

$$S_{78,1} = \alpha y^7 + (-\beta - 16\alpha)y^{11} + (14\beta + 120\alpha + 31616)y^{15} + (-560 - 91\beta + 4892160)y^{19} + \cdots,$$

with $\alpha = 0, 1, 2$ and $-448 \leqslant \beta \leqslant 0$, or

$$W_{78,2} = 1 + (3705 + 8\alpha)y^{14} + (71460 - 24\alpha)y^{16} + (658880 - 64\alpha)y^{18} + \cdots,$$

$$S_{78,2} = y^3 + (-\alpha - 135)y^{11} + (32960 + 14\alpha)y^{15} + (4885140 - 91\alpha)y^{19} + \cdots,$$

with $-468 \leqslant \alpha \leqslant -135$.

Known results on the binary self-dual $[78, 39, 14]$ codes are listed as follows.

- The existence of such codes with the weight enumerator of the form $W_{78,1}$ with $\alpha = 0$ and $\beta = -19$ was asserted in [1].
- It was shown in [22] that there are exactly six inequivalent double circulant self-dual $[78, 39, 14]$ codes. Five of them have weight enumerators of the form $W_{78,1}$ with $\alpha = 0$ and $\beta = 0$. The remaining one has weight enumerator of form $W_{78,1}$ with $\alpha = 0$ and $\beta = -78$.
- Gaborit and Otmani [20] constructed a code having weight enumerator of form $W_{78,1}$ with $\alpha = 0$ and $\beta = -26$.
- In [23], Gulliver, Harada, and Kim constructed more than 50 inequivalent codes. Among these codes, one has weight enumerator of form $W_{78,1}$ with $\alpha = 0$ and $\beta = -78$, one has weight enumerator of form $W_{78,2}$ with $\alpha = -135$, and all the others have weight enumerators of form $W_{78,1}$ with $\alpha = 0$ and $\beta = 0$.

We also summarize known results on binary self-dual $[116, 58, 18]$ codes.

- Gaborit and Otmani [20] constructed a self-dual $[116, 58, 18]$ code.
- Yorgova and Wassermann [45] found that there are at least 7 inequivalent self-dual $[116, 58, 18]$ codes with an automorphism of order 23.

In this paper, we investigate binary self-dual codes with a dihedral automorphism group D_{2p} of order $2p$, where p is an odd prime. The results will be applied to classify all binary self-dual $[78, 39, 14]$ codes with a dihedral automorphism group D_{38}. Some of these have weight enumerator of form $W_{78,1}$ with $\alpha = 0$ and $\beta = -38$ (the existence of such codes was previously unknown). Furthermore, we will show that there exist at least 141 inequivalent binary self-dual $[116, 58, 18]$ codes with dihedral automorphism group D_{58}. Since the order of the automorphism group is 58 for all of these codes, almost all of them are new up to equivalence.

In [8], Bouyuklieva and Willems introduced the definition of singly even self-dual codes with minimal shadow.

Definition 2. We say a self-dual code C of length $n = 24m + 8l + 2r$ with $l = 0, 1, 2$, $r = 0, 1, 2, 3$, is a code with minimal shadow if:

1. $wt(S) = r$ if $r > 0$; and
2. $wt(S) = 4$ if $r = 0$.

They proved that extremal self-dual codes of lengths $n = 24m + 2,\ 24m + 4,\ 24m + 6,\ 24m+10$, and $24m+22$ with minimal shadow do not exist. Moreover, they give explicit bounds in case the shadow is minimal. In this work, we consider extremal self-dual codes with near minimal and near near minimal shadow, and near extremal self-dual codes with minimal, near minimal, and near near minimal shadow and show nonexistence of such codes for certain parameters.

This paper is organized as follows. In Section 2 we first recall some results about binary self-dual codes having an automorphism of odd prime order. Then we extend these results to the case where the codes have dihedral automorphism group D_{2p}. In Section 3 we investigate self-dual $[78, 39, 14]$ codes with dihedral automorphism group D_{38} and $[116, 58, 18]$ codes with dihedral automorphism group D_{58}. In Section 4 we prove nonexistence of self-dual codes for certain parameters. Section 5 concludes the paper.

2 Preliminaries

Let C be a binary code with an automorphism σ of odd prime order p. If σ has c cycles of length p and f fixed points, we say that σ is of type $p-(c;f)$. Without loss of generality we may write

$$\sigma = \Omega_1 \cdots \Omega_c \Omega_{c+1} \cdots \Omega_{c+f},$$

where Ω_i is a p-cycle for $i = 1, 2, \cdots, c$, whereas for $i = c+1, \cdots, c+f$, Ω_i is a fixed point. Let $F_\sigma(C) = \{v \in C | v\sigma = v\}$ and $E_\sigma(C) = \{v \in C | \mathrm{wt}(v|_{\Omega_i}) \equiv 0 \pmod 2, i = 0, 1, \cdots, c+f\}$, where $v|_{\Omega_i}$ is the restriction of v to Ω_i. With this notation, we have the following lemma.

Lemma 3. *[29] $C = F_\sigma(C) \oplus E_\sigma(C)$.*

Clearly $v \in F_\sigma(C)$ if and only if $v \in C$ and v is constant on each cycle. Let $\pi : F_\sigma(C) \to \mathbb{F}_2^{c+f}$ denote the map defined by $\pi(v|_{\Omega_i}) = v_j$ for some $j \in \Omega_i$ and $i = 1, 2, \cdots, c+f$. Then $\pi(F_\sigma(C))$ is a binary self-dual code [29].

By deleting the last f coordinates of $E_\sigma(C)$, we obtain a new code, which is denoted by $E_\sigma(C)^*$. For $v \in E_\sigma(C)^*$ we identify $v|_{\Omega_i} = (v_0, v_1, \cdots, v_{p-1})$ with the polynomial $v_0 + v_1 x + \cdots + v_{p-1}x^{p-1}$ from P, where P is the set of even weight polynomials in $\mathbb{F}_2[x]/(x^p - 1)$. Thus we obtain the map $\varphi : E_\sigma(C)^* \to P^c$, where P^c denotes the module of all c-tuples over P. Clearly, $\varphi(E_\sigma(C)^*)$ is a submodule of the P-module P^c. If the multiplicative order of 2 modulo p is $p-1$, then the polynomial $1+x+x^2+\cdots+x^{p-1}$ of P is irreducible over $\mathbb{F}_2$. Hence P is an extension field of $\mathbb{F}_2$ with identity $e(x) = x + \cdots + x^{p-1}$ and the following result holds.

Lemma 4. *[43] Assume that the multiplicative order of 2 modulo p is $p-1$. Then a binary code C with an automorphism σ of odd prime order p is self-dual if and only if the following two conditions hold.*

(a) $\pi(F_\sigma(C))$ is a binary self-dual code of length $c+f$;

(b) $\varphi(E_\sigma(C)^*)$ is a self-dual code of length c over the field P under the inner product $u \cdot v = \sum_{i=1}^{c} u_i v_i^q$ for $q = 2^{\frac{p-1}{2}}$.

To classify the codes, we need additional conditions for equivalence and we use the following lemma.

Lemma 5. *[44] The following transformations applied to C lead to equivalent codes with automorphism σ:*

(a) a substitution $x \to x^t$ in $\varphi(E_\sigma(C)^*)$ where t is an integer, $1 \leqslant t \leqslant p-1$;

(b) a multiplication of any coordinate of $\varphi(E_\sigma(C)^*)$ by x^{t_j} where t_j is an integer, $0 \leqslant t_j \leqslant p-1$, $j = 1, 2, \cdots, c$;

(c) a permutation of the first c cycles of σ;

(d) a permutation of the last f coordinates of C.

The next definition gives an invariant of a code which was introduced by Dontcheva and Harada [15].

Definition 6. Let C be a binary self-dual $[n, k, d]$ code and $\{c_1, c_2, \cdots, c_m\}$ be the set of all codewords of weight d. The intersection numbers of the code C are defined as

$$I_j = \sharp\{(c_s, c_t) | \mathrm{dis}(c_s, c_t) = j, 1 \leqslant s < t \leqslant m\},$$

where $\mathrm{dis}(c_s, c_t)$ denotes the Hamming distance between c_s and c_t. Then I_j is an invariant under permutations of the coordinates.

The following two lemmas are efficient in excluding some types of automorphisms of a self-dual code.

Lemma 7. *[44] Let C be a binary self-dual $[n,k,d]$ code and let $\sigma \in Aut(C)$ be of type $p-(c;f)$, where p is an odd prime. If $g(s)=\sum_{i=0}^{s-1}\lceil \frac{d}{2^i}\rceil$, then*

(a) $pc \geqslant g(\frac{p-1}{2}c)$, and

(b) $f \geqslant g(\frac{f-c}{2})$ for $f > c$.

Lemma 8. *[7] Let C be a binary self-dual code of length n and let σ be an automorphism of C of type $p-(c;f)$, where p is an odd prime. If the multiplicative order of 2 modulo p is even, then c is even.*

In order to get our results, we give the following hypothesis.

Hypothesis 9. C is a binary self-dual $[n,n/2,d]$ code, where $n \geqslant 52$, $n=4p+f$, p is an odd prime number with 2 as a primitive root, $f=0,2,4$ and

$$d \geqslant \begin{cases} 4\lfloor \frac{n}{24}\rfloor + 2; \text{ if } n \not\equiv 22 \pmod{24}, \\ 4\lfloor \frac{n}{24}\rfloor + 4; \text{ if } n \equiv 22 \pmod{24}. \end{cases}$$

From Hypothesis 9, it is easy to see that $p \geqslant 13$ and $d \geqslant 10$. As a preparation, we have the following lemma.

Lemma 10. *Under Hypothesis 9, if C has an automorphism σ of type $p-(4;f)$, then $\varphi(E_\sigma(C)^*)$ is a self-dual $[4,2,3]$ code over the field $P \cong \mathbb{F}_{2^{p-1}}$.*

Proof. According to Lemma 4, $\varphi(E_\sigma(C)^*)$ is a self-dual $[4,2]$ code over the field $P \cong \mathbb{F}_{2^{p-1}}$. Since the minimum distance of $\varphi(E_\sigma(C)^*)$ cannot be 4, we only need to prove that $\varphi(E_\sigma(C)^*)$ has minimum distance $\neq 1,2$.

Case 1: $\varphi(E_\sigma(C)^*)$ has minimum weight 1.

Take $\mathbf{u} \in \varphi(E_\sigma(C)^*)$ with $\mathrm{wt}(\mathbf{u})=1$. Then we can assume that $\mathbf{u}=(v_1,0,0,0)$ with $v_1 \neq 0$. Since $(x+1)v_1^{-1}\mathbf{u}=(x+1,0,0,0) \in \varphi(E_\sigma(C)^*)$, we have $\mathrm{wt}(\varphi^{-1}((x+1)v_1^{-1}\mathbf{u}))=2$ which contradicts the fact $d \geqslant 10$.

Case 2: $\varphi(E_\sigma(C)^*)$ has minimum weight 2.

Take $\mathbf{u} \in \varphi(E_\sigma(C)^*)$ with $\mathrm{wt}(\mathbf{u})=2$. Suppose $\mathbf{u}=(v_1,v_2,0,0)$ with $v_1,v_2 \neq 0$. Let $U=\{v\mathbf{u} | v \in P\}$. Then $\dim_{\mathbb{F}_2} U = p-1$. Set $W=\varphi^{-1}(U) \subseteq E_\sigma(C)^*$. Let W^* be the code obtained from W by deleting the last $2p$ coordinates. Then W^* is a $[2p,p-1,d']$ code, where $d' \geqslant d$. To get a contradiction, take $g(s)=\sum_{i=0}^{s-1}\lceil \frac{d'}{2^i}\rceil$.

First we consider the case $p \equiv 1 \pmod 6$ and $f=0$. We can write $p=6k+1$, for some integer $k \geqslant 2$. Then $n=24k+4$, $d' \geqslant d \geqslant 4k+2$, $g(1) \geqslant 4k+2$, $g(2) \geqslant 6k+3$ and $g(3) \geqslant 7k+4$. If $2^l < 2k+1 \leqslant 2^{l+1}$ for $l \in \mathbb{N}$ then for $i > l$ we have $\frac{2k+1}{2^i} \leqslant 2^{l+1-i} \leqslant 1$

and therefore $\lceil \frac{2k+1}{2^i} \rceil = 1$. Hence

$$\begin{aligned} g(p-1) &\geqslant \sum_{i=0}^{p-2} \lceil \frac{4k+2}{2^i} \rceil \geqslant 7k+4+\sum_{i=2}^{p-3} \lceil \frac{2k+1}{2^i} \rceil \\ &= 7k+4+\sum_{i=2}^{l} \lceil \frac{2k+1}{2^i} \rceil + (p-3-l) \\ &= \sum_{i=2}^{l} \lceil \frac{2k+1}{2^i} \rceil + 12k+2+(k-l). \end{aligned}$$

If $k=2$, then $l=2$ and $g(p-1) > 12k+2$.

If $k=3$, then $l=2$ and $g(p-1) > 12k+2$.

If $k \geqslant 4$, then $l \geqslant 3$. Since $(k-l) > (2^{l-1} - l - \frac{1}{2}) > 0$, we get $g(p-1) > 12k+2$. Consequently, $g(p-1) > 12k+2 = 2p$ which contradicts the Griesmer Bound [31].

For the other cases of p and f, a similar discussion leads to a contradiction. Hence, $\varphi(E_\sigma(C)^*)$ can not have minimum weight 2. □

Now we are ready to prove our result.

Theorem 11. *Under Hypothesis 9, if C has a dihedral automorphism group D_{2p}, and $\sigma \in D_{2p}$ is an automorphism of type $p-(4;f)$ then $C = F_\sigma(C) \oplus E_\sigma(C)$, and there is a generator matrix of $\varphi(E_\sigma(C)^*)$ that has the form*

$$\operatorname{gen}(\varphi(E_\sigma(C)^*)) = \begin{bmatrix} b^{u_1} & 0 & a^{v_1} & a^{v_2}b^{u_3} \\ 0 & b^{u_2} & a^{v_2} & a^{v_1}b^{u_3} \end{bmatrix}, \tag{1}$$

where a, b are the elements of P of order $q-1$ and $\frac{q+1}{p}$, respectively. And $a^{v_1} + a^{v_2} = e$, $1 \leqslant v_1 < v_2 \leqslant q-2$, $0 \leqslant u_i \leqslant \frac{q+1}{p} - 1$ for $i = 1,2,3$, where $q = 2^{\frac{p-1}{2}}$. Also, the u_i's satisfy one of the following conditions:

1. $u_1 + u_2 \equiv u_3 \pmod{\frac{q+1}{p}}$;
2. $u_2 + u_3 \equiv u_1 \pmod{\frac{q+1}{p}}$;
3. $u_1 + u_3 \equiv u_2 \pmod{\frac{q+1}{p}}$;
4. $u_1 = u_2 = u_3 = 0$.

Proof. Suppose that C is a self-dual $[n, n/2, d]$ code with dihedral automorphism group D_{2p}. Let $\sigma \in D_{2p}$ be an automorphism of type $p-(4;f)$. Without loss of generality, we can write

$$\sigma = (1, \cdots, p)(p+1, \cdots, 2p)(2p+1, \cdots, 3p)(3p+1, \cdots, 4p).$$

Then $\varphi(E_\sigma(C)^*)$ is a self-dual $[4,2,3]$ code over the field P under the inner product $u\cdot v=\sum_{i=1}^{c}u_iv_i^q$ for $q=2^{\frac{p-1}{2}}$ by Lemma 10. Let e be the identity element of P, α a primitive element of P, and set $a=\alpha^{q+1}$ and $b=\alpha^{(q-1)p}$. Then by a computation similar to that in [44], we have

$$\mathrm{gen}(\varphi(E_\sigma(C)^*))=\begin{bmatrix} b^{u_1} & 0 & a^{v_1} & a^{v_2}b^{u_3}\\ 0 & b^{u_2} & a^{v_2} & a^{v_1}b^{u_3}\end{bmatrix}, \tag{2}$$

where $a^{v_1}+a^{v_2}=e$, $1\leqslant v_1<v_2\leqslant q-2$, and $0\leqslant u_i\leqslant\frac{q+1}{p}-1$ for $i=1,2,3$.

We consider the involution of D_{2p} acting on C. Let $\tau\in D_{2p}$ be an element of order 2 such that $\tau\sigma\tau=\sigma^{-1}$, that is

$$\begin{aligned}&(\tau(1),\cdots,\tau(p))(\tau(p+1),\cdots,\tau(2p))(\tau(2p+1),\cdots,\tau(3p))(\tau(3p+1),\cdots,\tau(4p))\\ &=(p,\cdots,1)(2p,\cdots,p+1)(3p,\cdots,2p+1)(4p,\cdots,3p+1).\end{aligned} \tag{3}$$

Then by Lemma 5(b)(d) we may relabel the coordinates so that $\tau\in S$ where S is the set consisting of the following elements:

$$(1,2p)\cdots(p,p+1)(2p+1,4p)\cdots(3p,3p+1),$$

$$(1,3p)\cdots(p,2p+1)(p+1,4p)\cdots(2p,3p+1),$$

$$(1,4p)\cdots(p,3p+1)(p+1,3p)\cdots(2p,2p+1),$$

$$(1,p)\cdots(\frac{p-1}{2},\frac{p+3}{2})(p+1,2p)\cdots(\frac{3p-1}{2},\frac{3p+3}{2})\cdots(3p+1,4p)\cdots(\frac{7p-1}{2},\frac{7p+3}{2}),$$

$$(1,p)\cdots(\frac{p-1}{2},\frac{p+3}{2})(p+1,2p)\cdots(\frac{3p-1}{2},\frac{3p+3}{2})(2p+1,4p)\cdots(3p,3p+1),$$

$$(1,p)\cdots(\frac{p-1}{2},\frac{p+3}{2})(p+1,3p)\cdots(2p,2p+1)(3p+1,4p)\cdots(\frac{7p-1}{2},\frac{7p+3}{2}),$$

$$(1,p)\cdots(\frac{p-1}{2},\frac{p+3}{2})(p+1,4p)\cdots(2p,3p+1)(2p+1,3p)\cdots(\frac{5p-1}{2},\frac{5p+1}{2}),$$

$$(1,2p)\cdots(p,p+1)(2p+1,3p)\cdots(\frac{5p-1}{2},\frac{5p+1}{2})(3p+1,4p)\cdots(\frac{7p-1}{2},\frac{7p+3}{2}),$$

$$(1,3p)\cdots(p,2p+1)(p+1,2p)\cdots(\frac{3p-1}{2},\frac{3p+3}{2})(3p+1,4p)\cdots(\frac{7p-1}{2},\frac{7p+3}{2}),$$

$$(1,4p)\cdots(p,3p+1)(p+1,2p)\cdots(\frac{3p-1}{2},\frac{3p+3}{2})(2p+1,3p)\cdots(\frac{5p-1}{2},\frac{5p+1}{2}).$$

We now consider the action of τ on $\varphi(E_\sigma(C)^*)$.

Let $-:\mathbb{F}_{2^{p-1}}\to\mathbb{F}_{2^{p-1}},x\to\overline{x}=x^q$ be the nontrivial Galois automorphism of $\mathbb{F}_{2^{p-1}}$ with fixed field $\mathbb{F}_q$.

Since the computation of each case is similar, we take $\tau=(1,2p)\cdots(p,p+1)(2p+1,4p)\cdots(3p,3p+1)$ as a sample. For the other cases, we just list the results.

The action of τ is given by

$$\tau(x_1, x_2, x_3, x_4) = (\overline{x_2}, \overline{x_1}, \overline{x_4}, \overline{x_3}),$$

where $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^{p-1}}$. So

$$\tau(\mathrm{gen}(\varphi(E_\sigma(C)^*))) = \begin{bmatrix} 0 & \overline{b}^{u_1} & a^{v_2}\overline{b}^{u_3} & a^{v_1} \\ \overline{b}^{u_2} & 0 & a^{v_1}\overline{b}^{u_3} & a^{v_2} \end{bmatrix}. \tag{4}$$

Since $\tau \in Aut(C)$, then $\sigma^{-1}(\tau(E_\sigma(C))) \subseteq C$, due to the orthogonality of the rows of matrices (2) and (4), we get the following equations

$$a^{v_1} + a^{v_2} = e,\ b^{u_1+u_2} + b^{u_3}a^{2v_1} + b^{u_3}a^{2v_2} = 0,$$

which imply that $u_1 + u_2 \equiv u_3 \pmod{\frac{q+1}{p}}$.

If $\tau = (1, 3p)\cdots(p, 2p+1)(p+1, 4p)\cdots(2p, 3p+1)$, then $u_2 + u_3 \equiv u_1 \pmod{\frac{q+1}{p}}$.

If $\tau = (1, 4p)\cdots(p, 3p+1)(p+1, 3p)\cdots(2p, 2p+1)$, then $u_1 + u_3 \equiv u_2 \pmod{\frac{q+1}{p}}$.

If $\tau = (1, p)\cdots(\frac{p-1}{2}, \frac{p+3}{2})(p+1, 2p)\cdots(\frac{3p-1}{2}, \frac{3p+3}{2})(2p+1, 3p)\cdots(\frac{5p-1}{2}, \frac{5p+1}{2})(3p+1, 4p)\cdots(\frac{7p-1}{2}, \frac{7p+3}{2}))$, then $u_1 = u_2 = u_3 = 0$.

In the other cases, there is no solution.

□

Remark 12. Our assumptions may seem restrictive, but they make for simple notations and are sufficient for our purposes.

3 New Optimal Self-Dual Codes with Dihedral Automorphism Group D_{2p}

3.1 Self-Dual [78, 39, 14] Codes with Dihedral Automorphism Group D_{38}

Theorem 13. *There are exactly* 16 *inequivalent self-dual* $[78, 39, 14]$ *codes with dihedral automorphism group* D_{38}*; they are listed in Table 1.*

Proof. Assume that C is a self-dual $[78, 39, 14]$ code having dihedral automorphism group D_{38} and let $\sigma \in D_{38}$ be an automorphism of order 19. It is easy to see that $19-(4;2)$ is the only possible type for σ by Lemmas 7 and 8. By Lemma 4, $\pi(F_\sigma(C))$ is a binary self-dual $[6, 3]$ code. Consequently,

$$\mathrm{gen}(\pi(F_\sigma(C))) = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}. \tag{5}$$

Let P be the vector space of even weight polynomials in $\mathbb{F}_2[x]/(x^{19}-1)$, e be the identity of P, $a = x + x^2 + x^5 + x^6 + x^{13} + x^{14} + x^{17} + x^{18}$, and $b = x^4 + x^7 + x^8 + x^9 +$

$x^{10}+x^{11}+x^{12}+x^{15}+x^{16}+x^{17}$. It is easy to verify that the multiplicative orders of a and b are 2^9-1 and $(2^9+1)/19$, respectively.

Since 2 is a primitive root of 19, it is easy to verify Hypothesis 9. By Theorem 11 there is a generator matrix of $\varphi(E_\sigma(C)^*)$ of the form

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{bmatrix} b^{u_1} & 0 & a^{v_1} & a^{v_2}b^{u_3} \\ 0 & b^{u_2} & a^{v_2} & a^{v_1}b^{u_3} \end{bmatrix}, \tag{6}$$

where $a^{v_1}+a^{v_2}=e$, $1 \leqslant v_1 < v_2 \leqslant 510$, $0 \leqslant u_i \leqslant 26$ for $i=1,2,3$, and the u_i's satisfy one of the following conditions:

1. $u_1+u_2 \equiv u_3 \pmod{27}$;
2. $u_2+u_3 \equiv u_1 \pmod{27}$;
3. $u_1+u_3 \equiv u_2 \pmod{27}$;
4. $u_1=u_2=u_3=0$.

From [16], we have $(v_1,v_2)\in V$, where $V=\{(1,93),(6,13),(7,505),(9,59),(15,37),(19,105),(20,99),(21,87),(25,251),(29,178),(31,193),(34,175),(39,111),(43,246),(45,61),(46,255),(49,119),(63,190),(73,219),(83,138),(91,167),(94,169),(103,108),(106,239),(114,221),(125,187),(155,213),(179,220),(191,242)\}$.

Let G be the automorphism group of the code generated by $\mathrm{gen}(\pi(F_\sigma(C)))$. Let S be the stabilizer of G on the set of fixed points $\{5,6\}$. Suppose s belongs to the symmetric group S_4. Then we use C^s to denote the self-dual code determined by E_σ and the matrix $\pi^{-1}(s(\mathrm{gen}(\pi(F_\sigma(C)))))$. By [32, Lemma 4.1], if s_1 and s_2 are permutations from the group S_4 and $Ss_1 = Ss_2$, then the codes C^{s_1} and C^{s_2} are equivalent. So in order to get all inequivalent self-dual $[78,39,14]$ codes with a dihedral automorphism group D_{38}, we must check $\pi^{-1}(s(\mathrm{gen}(\pi(F_\sigma(C)))))$, where $s \in S_4/S = \{I,(1,2,3,4),(1,2),(1,3)(2,4),(1,3,4),(1,4,3,2)\}$.

Now we consider the involution τ of D_{38} acting on $\pi^{-1}(s(\mathrm{gen}(\pi(F_\sigma(C)))))$.

If $\tau=(1,38)\cdots(19,20)(39,76)\cdots(57,58)$, an easy computation shows that s must be $(1,2,3,4)$.

Similarly, if $\tau=(1,57)\cdots(19,39)(20,76)\cdots(38,58)$, then $s\in\{(1,3,4),(1,2)\}$.

If $\tau=(1,76)\cdots(19,58)(20,57)\cdots(38,39)$, then $s\in\{I,(1,3)(2,4),(1,4,3,2)\}$.

If $\tau=(1,19)\cdots(9,11)(20,38)\cdots(28,30)(39,57)\cdots(47,49)(58,76)\cdots(66,68)$, then $s\in\{I,(1,2,3,4),(1,2),(1,3)(2,4),(1,3,4),(1,4,3,2)\}$.

Therefore, we should analyze the generator matrix

$$\mathrm{gen}(C) = \begin{bmatrix} \pi^{-1}(s(\mathrm{gen}(\pi(F_\sigma(C))))) \\ \mathrm{gen}(E_\sigma) \end{bmatrix}, \tag{7}$$

where $\mathrm{gen}(\pi(F_\sigma(C)))$ has been determined in (5) and $\mathrm{gen}(E_\sigma)$ corresponds to (6) with $(v_1,v_2)\in V$, $0\leqslant u_i \leqslant 26$ for $i=1,2,3$, and the u_i's $(i=1,2,3)$ and s satisfy one of the following conditions:

1. $u_1 + u_2 \equiv u_3 \pmod{27}, s = (1, 2, 3, 4)$;
2. $u_2 + u_3 \equiv u_1 \pmod{27}, s \in \{(1, 3, 4), (1, 2)\}$;
3. $u_1 + u_3 \equiv u_2 \pmod{27}, s \in \{I, (1, 3)(2, 4), (1, 4, 3, 2)\}$;
4. $u_1 = u_2 = u_3 = 0, s \in \{I, (1, 2, 3, 4), (1, 2), (1, 3)(2, 4), (1, 3, 4), (1, 4, 3, 2)\}$.

Using MAGMA [5], we found exactly 16 inequivalent self-dual $[78, 39, 14]$ codes with dihedral automorphism group D_{38}. Four of them have weight enumerator $W_{78,1}$ with $\alpha = 0$ and $\beta = -38$ which was unknown before. The corresponding values of the parameters are given in Table 1 (The explicit generator matrices for these self-dual codes can be found at http://www.math.zju.edu.cn/~ggn/selfdualcodes/Self-Dual-Codes.txt). All the codes have weight enumerators $W_{78,1}$ with $\alpha = 0$, so we just list the values of β. Here I_{28} is the intersection number. I is the identity permutation in the group S_4 and $\sharp$Aut denotes the order of the automorphism group of the corresponding code.

Since all the intersection numbers of the codes listed in Table 1 are different, they are inequivalent.

□

Table 1: Self-dual $[78, 39, 14]$ codes with dihedral automorphism group D_{38}

Code	u_1	u_2	u_3	v_1	v_2	s	β	I_{28}	$\sharp$Aut
C_1	6	15	21	1	93	$(1,2,3,4)$	0	646285	38
C_2	6	12	18	1	93	$(1,2,3,4)$	0	643910	38
C_3	10	10	0	215	335	$(1,3,4)$	0	644537	38
C_4	10	10	0	215	335	I	0	646266	38
C_5	10	13	3	29	178	I	0	643815	38
C_6	10	34	24	29	178	I	0	642428	38
C_7	29	9	20	35	231	$(1,3,4)$	0	642010	38
C_8	22	13	18	49	119	I	0	645107	38
C_9	25	21	4	83	138	$(1,3,4)$	0	650313	38
C_{10}	24	2	22	83	138	$(1,3,4)$	0	647254	38
C_{11}	20	25	22	83	138	$(1,3,4)$	0	645278	38
C_{12}	17	21	23	83	138	$(1,3,4)$	0	648546	38
C_{13}	26	6	5	9	59	$(1,2,3,4)$	-38	547523	38
C_{14}	21	12	6	19	105	$(1,2,3,4)$	-38	546573	38
C_{15}	21	15	9	19	105	$(1,2,3,4)$	-38	546649	38
C_{16}	15	5	17	29	178	I	-38	544882	38

Remark 14. It took about 5 hours on a 3 GHz CPU to classify the self-dual $[78, 39, 14]$ codes with a dihedral automorphism group D_{38}.

3.2 Self-Dual $[116, 58, 18]$ Codes with a Dihedral Automorphism Group D_{58}

Theorem 15. *There are at least* 141 *inequivalent self-dual* $[116, 58, 18]$ *codes with dihedral automorphism group* D_{58}*. They are listed in Table 5.*

Proof. Suppose C is a self-dual $[116, 58, 18]$ code with dihedral automorphism group D_{58} and let $\sigma \in D_{58}$ have order 29. A similar discussion to that in the previous subsection leads to

$$\mathrm{gen}(C) = \begin{bmatrix} \pi^{-1}(s(\mathrm{gen}(\pi(F_\sigma(C))))) \\ \mathrm{gen}(E_\sigma(C)) \end{bmatrix}, \tag{8}$$

where

$$\mathrm{gen}(\pi(F_\sigma(C))) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \tag{9}$$

$s \in S_4/S$, where S is the automorphism group of the code generated by $\mathrm{gen}(\pi(F_\sigma(C)))$, and $\mathrm{gen}(E_\sigma(C))$ corresponds to

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{bmatrix} b^{u_1} & 0 & a^{v_1} & a^{v_2}b^{u_3} \\ 0 & b^{u_2} & a^{v_2} & a^{v_1}b^{u_3} \end{bmatrix}, \tag{10}$$

with $a = x + x^3 + x^4 + x^6 + x^9 + x^{10} + x^{11} + x^{18} + x^{19} + x^{20} + x^{23} + x^{25} + x^{26} + x^{28} \in P$ of multiplicative order $2^{14} - 1$, $b = x + x^2 + x^3 + x^4 + x^6 + x^7 + x^{10} + x^{12} + x^{13} + x^{14} + x^{17} + x^{19} + x^{20} + x^{21} + x^{22} + x^{28} \in P$ of multiplicative order $(2^{14} + 1)/29$ and P being the set of all even weight polynomials in $\mathbb{F}_2[x]/(x^{29} - 1)$, $a^{v_1} + a^{v_2} = e$, $1 \leqslant v_1 < v_2 \leqslant 2^{14} - 2$ and $0 \leqslant u_i \leqslant 564$ for $i = 1, 2, 3$. The u_i's also satisfy one of the following conditions:

1. $u_1 + u_2 \equiv u_3 \pmod{565}$;
2. $u_2 + u_3 \equiv u_1 \pmod{565}$;
3. $u_1 + u_3 \equiv u_2 \pmod{565}$;
4. $u_1 = u_2 = u_3 = 0$.

Using MAGMA [5], we found at least 141 inequivalent self-dual $[116, 58, 18]$ codes with dihedral automorphism group D_{58}. The corresponding values of the parameters are given in Table 5 (The explicit generator matrices for these self-dual codes can be found at http://www.math.zju.edu.cn/~ggn/selfdualcodes/Self-Dual-Codes.txt). Here A_{18} denotes the number of codewords with weight 18, and I_{36} is the intersection number. I is the identity permutation in the group S_4 and $\sharp$Aut denotes the order of the automorphism group of the corresponding code.

It is easy to see that all the intersection numbers of the codes listed in Table 5 are different, hence they are inequivalent. Since all the automorphism groups have order 58, they are inequivalent with the codes constructed in [45].

□

4 Nonexistence of Some Self-Dual Codes

4.1 Some Restrictions on Weight Enumerators

In this section, we study the nonexistence of some singly even self-dual codes. According to [14], if C is a singly-even self-dual code of length $n = 24m + 8l + 2r$ with $l = 0, 1, 2$ and $r = 0, 1, 2, 3$, the weight enumerator of C and S are given by:

$$W(y) = \Sigma_{j=0}^{12m+4l+r} a_j y^{2j} = \Sigma_{i=0}^{3m+l} c_i (1 + y^2)^{12m+4l+r-4i} (y^2(1 - y^2)^2)^i,$$

$$S(y) = \Sigma_{j=0}^{6m+2l} b_j y^{4j+r} = \Sigma_{i=0}^{3m+l} (-1)^i c_i 2^{12m+4l+r-6i} y^{12m+4l+r-4i} (1 - y^4)^{2i}.$$

We can write the c_i as a linear combination of the a_i and as a linear combination of the b_i [36]:

$$c_i = \Sigma_{j=0}^{i} \alpha_{ij} a_j = \Sigma_{j=0}^{3m+l-i} \beta_{ij} b_j. \tag{11}$$

As a preparation, we give the definition of near minimal shadow and near near minimal shadow.

Definition 16. We say a self-dual code C of length $n = 24m + 8l + 2r$ with $l = 0, 1, 2$, $r = 0, 1, 2, 3$, is a code with near minimal shadow if:

1. $wt(S) = r + 4$ if $r > 0$; and
2. $wt(S) = 8$ if $r = 0$.

And a code with near near minimal shadow if:

1. $wt(S) = r + 8$ if $r > 0$; and
2. $wt(S) = 12$ if $r = 0$.

Then we have the following theorem.

Theorem 17. *An extremal self-dual code of length $n = 24m + 8l + 2r$ with near minimal shadow does not exist whenever:*

1. $r = 1$ *and* $l = 0$,
2. $r = 1$, $l = 1$ *and* $\frac{-12m+5}{-4m-2}\binom{5m+1}{m} - \frac{3m}{2m+1}\binom{5m}{m-1}$ *is not an integer,*
3. $r = 2$, $l = 0$ *and* $\frac{2(6m+1)(8m+1)}{16m(2m+1)}\binom{5m}{m-1} - \frac{3m-1}{2m+1}\binom{5m-1}{m-2}$ *is not an integer,*
4. $r = 3$, $l = 0$ *and* $\frac{3(4m+1)(6m+1)}{8m(2m+1)}\binom{5m}{m-1} - \frac{3m-1}{2m+1}\binom{5m-1}{m-2}$ *is not an integer.*

Proof. Suppose C is an extremal singly even self-dual code of length $n = 24m + 8l + 2r$ with near minimal shadow, where $r > 0$. Then $d = 4m + 4$, $wt(S) = r + 4$, $a_0 = 1$ and $a_1 = \cdots = a_{2m+1} = 0$.

By Theorem 1, if $r > 0$ we have $b_0 = 0$, $b_1 = 1$ and $b_2 = b_3 = \cdots = b_{m-2} = 0$ for $m \geqslant 1$.

For the case when $r = 1$ and $l = 0$, if $b_{m-1} \neq 0$ then there must exist some u in S with $wt(u) = 4m - 3$ as well as some v in S with $wt(v) = 5$. But then we have $u + v \in C$ with $wt(u + v) \leqslant 4m + 2$, a contradiction to the minimum weight of C. Then we must have $b_{m-1} = 0$. Then by (11) we have

$$c_{2m+1} = \alpha_{2m+1,0} = \beta_{2m+1,1} + \Sigma_{j=m}^{m-1} \beta_{2m+1,j} b_j.$$

This gives us $c_{2m+1} = \alpha_{2m+1,0} = \beta_{2m+1,1}$. The α_{ij} and β_{ij} were computed in [8] and so we get

$$-\frac{(12m+1)(56m+4)}{(2m+1)(m-1)} \binom{5m-1}{m-2} = -2^5 \frac{3m-1}{2m+1} \binom{5m-1}{m-2},$$

which has no integer solution.

For the case when $r = 1$ and $l = 1$, again we must have $b_{m-1} = 0$. Then (11) gives us

$$\alpha_{2m+1,0} = \beta_{2m+1,1} + \beta_{2m+1,m} b_m,$$

and so

$$b_m = \frac{\alpha_{2m+1,0} - \beta_{2m+1,1}}{\beta_{2m+1,m}} = \frac{-12m+5}{-4m-2} \binom{5m+1}{m} - \frac{3m}{2m+1} \binom{5m}{m-1}, \tag{12}$$

which must be an integer for such a code to exist.

For the case when $r = 2$ and $l = 0$ we have $b_2 = b_3 = \cdots = b_{m-2} = 0$ and from (11) we get

$$\alpha_{2m+1,0} = \beta_{2m+1,1} + \beta_{2m+1,m-1} b_{m-1},$$

and so

$$b_{m-1} = \frac{\alpha_{2m+1,0} - \beta_{2m+1,1}}{\beta_{2m+1,m-1}} = \frac{2(6m+1)(8m+1)}{16m(2m+1)} \binom{5m}{m-1} - \frac{3m-1}{2m+1} \binom{5m-1}{m-2}, \tag{13}$$

which must be an integer for such a code to exist.

When $r = 3$ and $l = 0$, we have $b_2 = b_3 = \cdots = b_{m-2} = 0$ and from (11) we get

$$\alpha_{2m+1,0} = \beta_{2m+1,1} + \beta_{2m+1,m-1} b_{m-1},$$

which gives

$$b_{m-1} = \frac{\alpha_{2m+1,0} - \beta_{2m+1,1}}{\beta_{2m+1,m-1}} = \frac{3(4m+1)(6m+1)}{8m(2m+1)} \binom{5m}{m-1} - \frac{3m-1}{2m+1} \binom{5m-1}{m-2}, \tag{14}$$

which must be an integer for such a code to exist. $\square$

For the near extremal self-dual code, we have a similar result.

Theorem 18. *A near extremal self-dual code with minimal shadow does not exist whenever:*

1. $r = 1$, $l = 0$ *and* $\frac{24m+2}{m}\binom{5m-1}{m-1} - \frac{3}{2}\binom{5m-1}{m}$ *is not an integer,*
2. $r = 2$, $l = 0$ *and* $\frac{24m+4}{m}\left[\binom{5m}{m-2} + 3\binom{5m+1}{m-2}\right] - \frac{3}{2}\binom{5m-1}{m}$ *is not an integer.*

Proof. Let C be a near extremal self-dual code of length $n = 24m + 8l + 2r$ with minimal shadow, where $r > 0$. Then we have $d = 4m + 2$, $wt(S) = r$, $a_0 = 1$ and $a_1 = a_2 = \cdots = a_{2m} = 0$.

Since $r > 0$, then by Theorem 1, we have $b_0 = 1$ and $b_1 = b_2 = \cdots = b_{m-2} = 0$ for $m \geqslant 1$, otherwise there will be v in S with $wt(v) \leqslant 4m - 8 + r$, and u in S with $wt(u) = r$ so that $u + v$ is in C and $wt(u + v) \leqslant 4m - 8 + 2r \leqslant 4m - 2$, a contradiction to the minimum weight of C.

Now suppose $r = 1, 2$ and $l = 0$. If $b_{m-1} \neq 0$ there will be u and v in S with $wt(u + v) \leqslant 4m - 3 + r \leqslant 4m$, a contradiction to the minimum weight of C. Then $b_{m-1} = 0$. From (11) we have

$$\alpha_{2m,0} = \beta_{2m,0} + \beta_{2m,m}.$$

According to [36] we have

$$\begin{aligned}
\alpha_{2m}(24m + 2r) &= -\frac{12m + r}{2m}[\text{coeff. of } y^{2m-1} \text{ in } (1 + y)^{-4m-r-1}(1 - y)^{-4m}] \\
&= -\frac{12m + r}{2m}[\text{coeff. of } y^{2m-1} \text{ in } (1 + y)^{-r-1}(1 - y^2)^{-4m}] \\
&= -\frac{12m + r}{2m}[\text{coeff. of } y^{2m-1} \text{ in } (1 - y^2)^{-4m-r-1}(1 - y)^{r+1}] \\
&= -\frac{12m + r}{2m}[\text{coeff. of } y^{2m-1} \text{ in } (1 - y)\Sigma_{j=0}^{m}\binom{4m + r + j}{j} y^{2j}] \\
&= \begin{cases} -\frac{12m+1}{m}\binom{5m-1}{m-1}; & \text{if } r = 1, \\ \frac{6m+1}{m}[\binom{5m}{m-2} + 3\binom{5m+1}{m-1}]; & \text{if } r = 2. \end{cases}
\end{aligned}$$

We also have $\beta_{2m,0} = 2^{-r}\frac{3}{2}\binom{5m-1}{m}$ and $\beta_{2m,m} = 2^{-r}$. Then if $r = 1$, (11) gives us

$$b_m = \frac{24m + 2}{m}\binom{5m - 1}{m - 1} - \frac{3}{2}\binom{5m - 1}{m}, \tag{15}$$

which must be an integer for such a code to exist, and if $r = 2$, (11) gives us

$$b_m = \frac{24m + 4}{m}\left[\binom{5m}{m - 2} + 3\binom{5m + 1}{m - 2}\right] - \frac{3}{2}\binom{5m - 1}{m}, \tag{16}$$

which must also be an integer for a code to exist. ☐

If C is an extremal self-dual code of length $24m + 8l + 2r$ with near near minimal shadow we get by a similar argument as above that

$$b_{m-1} = 2^{-5} \frac{(12m+1)(56m+4)}{(2m+1)(m-1)} \binom{5m-1}{m-2},$$

whence the following.

Theorem 19. *An extremal self-dual code of length $24m+8l+2r$ with near near minimal shadow does not exist whenever $r = 1$ and $l = 0$ and $2^{-5}\frac{(12m+1)(56m+4)}{(2m+1)(m-1)}\binom{5m-1}{m-2}$ is not an integer.*

We will also make use of the following lemma, which was originally proved by Ray-Cahaudhuri and Wilson in [38].

Lemma 20. *Let X be a set of cardinality v. For $s \leqslant k \leqslant v - s$ let $\mathfrak{B}$ be a collection of subsets of X each having cardinality k and having the property that, for $B, B' \in \mathfrak{B}$, $B \neq B'$, the cardinality of $B \cap B'$ takes only s distinct values. Then $|\mathfrak{B}| \leqslant \binom{v}{s}$.*

Remark 21. Let C be a self-dual code of length $n = 24m+8l+2r$ with $m \geqslant 2$ not having minimal shadow, let $s := wt(S)$ and denote the set of vectors of S of minimum weight by B_s. Suppose that $2s - d \leqslant 2$. It follows that if u and v are members of B_s, then $wt(u \cap v) \leqslant 1$. If $2s - d = 2$ then the members of S of minimum weight can intersect in either 0 or 1 nonzero coordinate positions. Because of the orthogonality relations among the cosets of C_0 in $C_0^{\perp}$, i.e. since $C_1 \perp C_3$ and $C_i \not\perp C_i$ for $i = 1, 3$, we have any two members of C_i intersecting in one nonzero coordinate position for $i = 1, 2$. We also have that if $u \in C_1$ and $v \in C_3$ then $wt(u \cap v) = 0$. Let $\mathfrak{B}_i$ be the set of vectors in C_i of weight s. Then we have $\mathfrak{B}_1$ and $\mathfrak{B}_3$ are disjoint. Let m_i be the effective length of $\mathfrak{B}_i$. Then by Lemma 20 we have $B_s \leqslant m_1 + m_3 \leqslant n$.

4.2 Application to Self-Dual Codes of Lengths 74, 76, 82, 98, and 100

In [18] several weight enumerators are computed for binary singly even self-dual codes of length n for $66 \leqslant n \leqslant 100$. For each length they give a combination of weight enumerators for that of a code with minimal, near minimal, and near near minimal shadow. We have eliminated several of the possibilities by using (12)-(16) either to show the value is not an integer, or that it does not agree with the value computed in [18]. For $n = 74$ and $n = 98$ we get resp. $5447/3$ and $38301/2$ as the value b_m and so Part 1 of Theorem 18 applies. For $n = 76,\ 82,\ 100$ we use resp. (16), (12), (16) to get values (Table 4) that do not agree with those given in [18], which were computed using the method introduced by Conway and Sloane in [14]. We also use the comment following Lemma 20 to narrow the possible range for the parameter in the near near extremal weight enumerators for cases $n = 82$ and 100. These restrictions are summarized in Tables 2 and 3 below.

We now list the possible weight enumerators of extremal and near extremal singly even self-dual codes of lengths $n = 74,\ 76,\ 82,\ 98$, and 100.

Table 2: Summary of restrictions on possible weight enumerator for lengths $74, 76, 82, 98, 100$

n	Weight Enumerator Eliminated	b_m	Reference
74	Minimal Shadow	5447/3	Part 1 of Theorem 18
76	Minimal Shadow	1050	Equation (16)
82	Near Minimal Shadow	1105	Equation (12)
98	Minimal Shadow	38301/2	Part 1 of Theorem 18
100	Minimal Shadow	14686	Equation (12)

Table 3: Summary of restrictions on possible range for α, β in the near near minimal shadow case for lengths $82, 100$

n	New range for α, β	Reference
82	$0 \leqslant \alpha \leqslant 82$	Remark 21
100	$0 \leqslant \alpha \leqslant min\{100, -\frac{1}{20}\beta\}$ where $-3265 \leqslant \beta \leqslant 0$	Remark 21

- The possible weight enumerators for self-dual $[74, 37, 14]$ codes are

$$\begin{cases} S_1 = -\alpha y^9 + (2590 + 14\alpha)y^{13} + (674584 - 91\alpha)y^{17} + (364\alpha + 44035772)y^{21} + \cdots, \\ W_1 = 1 + (6364 + 32\alpha)y^{14} + (100603 - 160\alpha)y^{16} + (32\alpha + 1061678)y^{18} + \cdots, \\ (-185 \leqslant \alpha \leqslant 0), \end{cases}$$

  and

$$\begin{cases} S_2 = y^5 + (-16 - \alpha)y^9 + (2710 + 14\alpha)y^{13} + (674024 - 91\alpha)y^{17} + \cdots, \\ W_2 = 1 + (6346 + 320\alpha)y^{14} + (102651 - 160\alpha)y^{16} + (32\alpha + 1039150)y^{18} + \cdots, \\ (-19 \leqslant \alpha \leqslant -16). \end{cases}$$

  The weight enumerator for the minimal shadow case was eliminated in this paper. There is no known code for either case.

- The possible weight enumerators for self-dual $[76, 38, 14]$ codes are

$$\begin{cases} S_1 = \alpha y^{10} + (9500 - 14\alpha)y^{14} + (1831600 + 91\alpha)y^{18} + (105689400 - 364\alpha)y^{22} + \cdots, \\ W_1 = 1 + (4750 - 16\alpha)y^{14} + (79895 + 64\alpha)y^{16} + (64\alpha + 915800)y^{18} + \cdots, \\ (0 \leqslant \alpha \leqslant 296), \end{cases}$$

  and

$$\begin{cases} S_2 = y^6 + (-16 - \alpha)y^{10} + (9620 + 14\alpha)y^{14} + (1831040 - 91\alpha)y^{18} + \cdots, \\ W_2 = 1 + (4750 + 16\alpha)y^{14} + (80919 - 64\alpha)y^{16} + (905560 - 64\alpha)y^{18} + \cdots, \\ (-296 \leqslant \alpha \leqslant -16). \end{cases}$$

Table 4: Contradictory values of b_m for cases $n = 76, 82$ and 100

n	b_m computed using above method	b_m computed using method of [14]
76	1050	2590
82	1105	1505
100	14686	98686

The weight enumerator for the minimal shadow case was eliminated in this paper. In [1], a code with weight enumerator W_1 for $\alpha = 0$ was constructed by assuming an automorphism of order 19. It is shown in [16] that there are exactly three inequivalent self-dual $[76, 38, 14]$ codes having an automorphism of order 19. All of these have weight enumerator W_1 with $\alpha = 0$.

- The possible weight enumerator for self-dual $[82, 41, 16]$ codes is

$$\begin{cases} S_1 = \alpha y^9 + (1640 - \alpha)y^{13} + (281424 + 120\alpha)y^{17} + (-560\alpha + 33442552)y^{21} + \cdots, \\ W_1 = 1 + (39524 + 128\alpha)y^{16} + (556985 - 896\alpha)y^{18} + (1536\alpha + 5628480)y^{20} + \cdots, \\ (0 \leqslant \alpha \leqslant 82). \end{cases}$$

The weight enumerator for the near minimal shadow case was eliminated, and the range for the parameter in the near near minimal shadow case was improved in this paper. There is no known code with this weight enumerator.

- The possible weight enumerators for self-dual $[98, 49, 18]$ codes are

$$\begin{cases} S_1 = \alpha y^9 + (-\beta - 20\alpha)y^{13} + (190\alpha + 18\beta + 27930)y^{17} + \cdots, \\ W_1 = 1 + (70756 + 32\beta)y^{18} + (2048\alpha + 1256752 - 160\beta)y^{20} + \cdots, \\ (0 \leqslant \alpha \leqslant min\{2, \frac{1}{20}\beta\} \text{ where } 0 \leqslant \beta \leqslant 2211), \end{cases}$$

and

$$\begin{cases} S_2 = y^5 + (-209 - \alpha)y^{13} + (30570 + 18\alpha)y^{17} + (9101051 - 153\alpha)y^{21} + \cdots, \\ W_2 = 1 + (70756 + 32\alpha)y^{18} + (1301808 - 16\alpha)y^{20} + (-96\alpha + 15231280)y^{22} + \cdots, \\ (-1698 \leqslant \alpha \leqslant -209). \end{cases}$$

The weight enumerator for the minimal shadow case was eliminated in this paper. The range for the parameter in the near near minimal shadow case was improved in [27]. There is no known code for either case.

- The possible weight enumerators for self-dual $[100, 50, 18]$ codes are

$$\begin{cases} S_1 = \alpha y^{10} + (-\beta - 20\alpha)y^{14} + (18\beta + 104500 - 190\alpha)y^{18} + \cdots, \\ W_1 = 1 + (16\beta + 52250)y^{18} + (972180 - 64\beta + 1024\alpha)y^{20} + \cdots, \\ (0 \leqslant \alpha \leqslant min\{100, -\frac{1}{20}\beta\} \text{ where } -3265 \leqslant \beta \leqslant 0), \end{cases}$$

and

$$\begin{cases} S_2 = y^6 + (-209-\alpha)y^{14} + (107140+18\alpha)y^{18} + (26137435-153\alpha)y^{22} + \cdots, \\ W_2 = 1 + (52250+16\alpha)y^{18} + (994708-64\alpha)y^{20} + (-128\alpha+12786784)y^{22} + \cdots, \\ (-5952 \leqslant \alpha \leqslant -209). \end{cases}$$

The weight enumerator for the near minimal shadow case was eliminated, and the range for the parameter in the near near minimal shadow case was improved in this paper. There is no known code for either case.

5 Conclusion

This paper demonstrates some results on self-dual codes. We make two contributions to this topic. The first one is the decomposition of binary self-dual $[4p+f, 2p+\frac{f}{2}, d]$ $(f = 0, 2, 4)$ codes with dihedral automorphism group D_{2p}, where p is an odd prime. These results are applied to classify self-dual $[78, 39, 14]$ codes with dihedral automorphism group D_{38} and we obtain some self-dual codes with new weight enumerators. Furthermore, we also show that there are at least 141 inequivalent self-dual $[116, 58, 18]$ codes with dihedral automorphism group D_{58}. Up to equivalence, most of these codes are new since the orders of the automorphism groups of all but one known self-dual $[116, 58, 18]$ code are divisible by 23. The second one is the restriction on the extremal self-dual codes with near minimal shadow, and near extremal self-dual codes with minimal, near minimal, and near near minimal shadow. And using these results, we eliminate some of the possible weight enumerators of self-dual codes with lengths 74, 76, 82, 98 and 100 determined in [14] and [18]. Self-dual codes with these weight enumerators have been constructed only for the length 76 [16], [1]. Constructing the self-dual codes with these weight enumerators of other lengths seems to be a challenging problem.

Table 5: Self-dual $[116, 58, 18]$ codes with dihedral automorphism group D_{58}

Code	u_1	u_2	u_3	v_1	v_2	s	A_{18}	I_{36}	$\sharp$Aut
C_1	9	153	144	882	12183	$(2,3,4)$	2146	178205	58
C_2	37	8	29	882	12183	I	2378	209989	58
C_3	14	259	273	259	15951	$(2,3,4)$	2610	260391	58
C_4	21	34	55	259	15951	$(2,3,4)$	2784	287912	58
C_5	3	200	203	259	15951	$(1,2,3,4)$	2842	301397	58
C_6	116	85	31	259	15951	$(1,2,3,4)$	2842	307081	58
C_7	13	189	176	882	12183	$(2,3,4)$	2842	300556	58
C_8	14	132	118	882	12183	I	2842	305196	58
C_9	28	134	106	259	15951	$(2,3,4)$	2842	299396	58
C_{10}	2	138	140	882	12183	$(1,2,3,4)$	2900	313287	58

Table 5 *Continued*

Code	u_1	u_2	u_3	v_1	v_2	s	A_{18}	I_{36}	$\sharp$Aut
C_{11}	19	99	118	882	12183	$(1,2,3,4)$	2900	318565	58
C_{12}	19	99	118	882	12183	$(2,3,4)$	2900	310880	58
C_{13}	13	145	158	259	15951	$(1,2,3,4)$	2900	306066	58
C_{14}	37	33	4	882	12183	I	2900	312417	58
C_{15}	1	156	155	882	12183	$(2,3,4)$	2900	315549	58
C_{16}	29	143	172	882	12183	$(1,2,3,4)$	2958	325119	58
C_{17}	23	169	146	882	12183	$(2,3,4)$	2958	327410	58
C_{18}	17	39	56	882	12183	$(2,3,4)$	3016	343360	58
C_{19}	272	245	27	5469	9024	$(1,2,3,4)$	3016	342171	58
C_{20}	44	39	5	259	15951	I	3016	340547	58
C_{21}	5	234	229	882	12183	$(2,3,4)$	3016	341620	58
C_{22}	21	120	99	882	12183	$(2,3,4)$	3016	337995	58
C_{23}	5	150	155	5469	9024	$(1,2,3,4)$	3074	342983	58
C_{24}	29	200	229	882	12183	$(2,3,4)$	3074	358933	58
C_{25}	14	96	110	259	15951	$(2,3,4)$	3074	348174	58
C_{26}	97	67	30	882	12183	I	3074	356903	58
C_{27}	10	167	157	5469	9024	I	3074	348377	58
C_{28}	5	279	284	882	12183	$(2,3,4)$	3132	361717	58
C_{29}	10	83	93	5469	9024	$(2,3,4)$	3132	372186	58
C_{30}	39	317	278	882	12183	$(2,3,4)$	3132	368793	58
C_{31}	31	25	6	882	12183	I	3132	359716	58
C_{32}	16	20	4	882	12183	$(2,3,4)$	3132	367169	58
C_{33}	2	265	267	259	15951	$(2,3,4)$	3190	381495	58
C_{34}	27	83	110	259	15951	$(1,2,3,4)$	3190	371809	58
C_{35}	35	14	49	259	15951	$(1,2,3,4)$	3190	374593	58
C_{36}	36	134	170	259	15951	$(2,3,4)$	3190	381031	58
C_{37}	198	185	13	5469	9024	I	3190	382916	58
C_{38}	44	29	15	882	12183	I	3190	373375	58
C_{39}	136	105	31	259	15951	$(1,2,3,4)$	3190	382568	58
C_{40}	9	189	180	5469	9024	I	3190	378276	58
C_{41}	10	167	157	5469	9024	$(2,3,4)$	3190	382104	58
C_{42}	12	259	247	5469	9024	$(2,3,4)$	3190	391123	58
C_{43}	22	166	188	5469	9024	$(2,3,4)$	3248	388455	58
C_{44}	42	16	58	882	12183	$(2,3,4)$	3248	386280	58
C_{45}	3	200	203	259	15951	$(2,3,4)$	3248	396778	58
C_{46}	201	180	21	259	15951	$(1,2,3,4)$	3248	389847	58
C_{47}	12	259	247	5469	9024	I	3248	391645	58
C_{48}	13	189	176	882	12183	I	3248	392022	58
C_{49}	4	172	176	5469	9024	$(1,2,3,4)$	3306	406522	58
C_{50}	40	217	257	5469	9024	$(1,2,3,4)$	3306	408958	58

Table 5 *Continued*

Code	u_1	u_2	u_3	v_1	v_2	s	A_{18}	I_{36}	♯Aut
C_{51}	40	217	257	5469	9024	$(2,3,4)$	3306	408697	58
C_{52}	44	29	15	882	12183	$(1,2,3,4)$	3306	398750	58
C_{53}	9	153	144	882	12183	I	3306	412119	58
C_{54}	21	120	99	882	12183	I	3306	412554	58
C_{55}	23	169	146	882	12183	I	3306	404434	58
C_{56}	5	279	284	882	12183	I	3335	412815	58
C_{57}	10	83	93	5469	9024	$(1,2,3,4)$	3364	417890	58
C_{58}	22	166	188	5469	9024	$(1,2,3,4)$	3364	413830	58
C_{59}	29	200	229	882	12183	$(1,2,3,4)$	3364	417165	58
C_{60}	208	198	10	5469	9024	I	3364	428098	58
C_{61}	272	245	27	5469	9024	I	3364	425778	58
C_{62}	5	234	229	882	12183	I	3364	423777	58
C_{63}	2	138	140	882	12183	$(2,3,4)$	3422	435812	58
C_{64}	6	172	278	882	12183	$(1,2,3,4)$	3422	428939	58
C_{65}	39	272	311	5469	9024	$(2,3,4)$	3422	442511	58
C_{66}	42	55	97	882	12183	$(1,2,3,4)$	3422	438045	58
C_{67}	125	122	3	5469	9024	I	3422	442395	58
C_{68}	17	49	66	5469	9024	$(2,3,4)$	3480	449007	58
C_{69}	42	55	97	882	12183	$(2,3,4)$	3480	452284	58
C_{70}	2	265	267	259	15951	$(1,2,3,4)$	3480	445556	58
C_{71}	27	83	110	259	15951	$(2,3,4)$	3480	458200	58
C_{72}	184	165	19	5469	9024	I	3480	454778	58
C_{73}	140	118	22	5469	9024	I	3480	447992	58
C_{74}	37	8	29	882	12183	$(1,2,3,4)$	3480	447325	58
C_{75}	5	150	155	5469	9024	$(2,3,4)$	3538	470641	58
C_{76}	34	227	263	882	12183	$(2,3,4)$	3538	464638	58
C_{77}	44	237	281	882	12183	$(1,2,3,4)$	3538	464928	58
C_{78}	14	132	118	882	12183	$(2,3,4)$	3538	463594	58
C_{79}	210	190	20	882	12183	I	3596	484010	58
C_{80}	91	63	28	259	15951	$(1,2,3,4)$	3596	475455	58
C_{81}	9	189	180	5469	9024	$(2,3,4)$	3596	486214	58
C_{82}	1	156	155	882	12183	I	3596	478645	58
C_{83}	39	272	311	5469	9024	$(1,2,3,4)$	3654	489346	58
C_{84}	34	227	263	882	12183	$(1,2,3,4)$	3654	495581	58
C_{85}	44	237	281	882	12183	$(2,3,4)$	3654	494943	58
C_{86}	14	259	273	259	15951	$(1,2,3,4)$	3654	495900	58
C_{87}	125	122	3	5469	9024	$(1,2,3,4)$	3654	509820	58
C_{88}	184	165	19	5469	9024	$(1,2,3,4)$	3654	497089	58
C_{89}	210	190	20	882	12183	$(2,3,4)$	3683	516171	58
C_{90}	21	34	55	259	15951	I	3712	499264	58

Table 5 *Continued*

Code	u_1	u_2	u_3	v_1	v_2	s	A_{18}	I_{36}	$\sharp$Aut
C_{91}	35	14	49	259	15951	$(2,3,4)$	3712	509095	58
C_{92}	140	118	22	5469	9024	$(1,2,3,4)$	3712	509588	58
C_{93}	31	25	6	882	12183	$(1,2,3,4)$	3712	519970	58
C_{94}	201	180	21	259	15951	I	3712	516084	58
C_{95}	136	105	31	259	15951	I	3712	519390	58
C_{96}	39	278	317	882	12183	$(1,2,3,4)$	3770	526727	58
C_{97}	42	16	58	882	12183	$(1,2,3,4)$	3770	528757	58
C_{98}	208	198	10	5469	9024	$(2,3,4)$	3770	527017	58
C_{99}	15	2	13	882	12183	I	3770	536500	58
C_{100}	4	172	176	5469	9024	$(2,3,4)$	3828	546853	58
C_{101}	116	85	31	259	15951	I	3828	539255	58
C_{102}	6	272	278	882	12183	I	3915	565529	58
C_{103}	14	96	110	259	15951	I	3944	572228	58
C_{104}	208	198	10	5469	9024	$(1,2,3,4)$	3944	581392	58
C_{105}	17	49	66	5469	9024	$(1,2,3,4)$	4002	588816	58
C_{106}	184	165	19	5469	9024	$(2,3,4)$	4002	598444	58
C_{107}	16	20	4	882	12183	I	4002	605346	58
C_{108}	6	272	278	882	12183	$(2,3,4)$	4060	605201	58
C_{109}	17	39	56	882	12183	$(1,2,3,4)$	4060	616279	58
C_{110}	14	96	110	259	15951	$(1,2,3,4)$	4060	616047	58
C_{111}	15	2	13	882	12183	$(1,2,3,4)$	4060	606941	58
C_{112}	36	134	170	259	15951	$(1,2,3,4)$	4118	635274	58
C_{113}	125	122	3	5469	9024	$(2,3,4)$	4147	632026	58
C_{114}	39	278	317	882	12183	I	4176	645511	58
C_{115}	299	273	26	5469	9024	I	4176	636724	58
C_{116}	37	33	4	882	12183	$(1,2,3,4)$	4176	647309	58
C_{117}	34	227	263	882	12183	I	4205	658155	58
C_{118}	13	145	158	259	15951	$(2,3,4)$	4234	686082	58
C_{119}	97	67	30	882	12183	$(1,2,3,4)$	4234	661722	58
C_{120}	44	39	5	259	15951	$(1,2,3,4)$	4234	672278	58
C_{121}	4	172	176	5469	9024	I	4292	684951	58
C_{122}	42	16	58	882	12183	I	4292	678803	58
C_{123}	15	2	13	882	12183	$(2,3,4)$	4292	691592	58
C_{124}	210	190	20	882	12183	$(1,2,3,4)$	4292	677585	58
C_{125}	35	14	49	259	15951	I	4321	692114	58
C_{126}	29	143	172	882	12183	$(2,3,4)$	4350	715169	58
C_{127}	198	185	13	5469	9024	$(1,2,3,4)$	4408	730046	58
C_{128}	13	145	158	259	15951	I	4437	725377	58
C_{129}	198	185	13	5469	9024	$(2,3,4)$	4437	736078	58
C_{130}	31	25	6	882	12183	$(2,3,4)$	4553	764933	58

Table 5 *Continued*

Code	u_1	u_2	u_3	v_1	v_2	s	A_{18}	I_{36}	$\sharp$Aut
C_{131}	12	259	247	5469	9024	$(1,2,3,4)$	4553	784682	58
C_{132}	28	134	106	259	15951	I	4582	778360	58
C_{133}	5	279	284	882	12183	$(1,2,3,4)$	4698	817713	58
C_{134}	29	200	229	882	12183	I	4698	827718	58
C_{135}	116	85	31	259	15951	$(2,3,4)$	4698	818554	58
C_{136}	36	134	170	259	15951	I	4756	838100	58
C_{137}	299	273	26	5469	9024	$(2,3,4)$	4785	857124	58
C_{138}	21	34	55	259	15951	$(1,2,3,4)$	4872	869536	58
C_{139}	37	33	4	882	12183	$(2,3,4)$	4872	879715	58
C_{140}	3	200	203	259	15951	I	5075	947343	58
C_{141}	27	83	110	259	15951	I	5220	1005807	58

Acknowledgements

The authors express their gratitude to the anonymous reviewer for his comments which improve the presentation of this paper, and to Prof. Q. Xiang, the editor-in-chief, for his excellent editorial job.

References

[1] A. Baartmans and V. Yorgov. Some new extremal codes of lengths 76 and 78. *IEEE Trans. Inform. Theory*, 49(5):1353–1354, 2003.

[2] K. Betsumiya, M. Harada, and A. Munemasa. A complete classification of doubly even self-dual codes of length 40. *Electron. J. Combin.*, 19(3):#P18, 12, 2012.

[3] R. T. Bilous. Enumeration of the binary self-dual codes of length 34. *J. Combin. Math. Combin. Comput.*, 59:173–211, 2006.

[4] R. T. Bilous and G. H. J. van Rees. An enumeration of binary self-dual codes of length 32. *Des. Codes Cryptogr.*, 26(1-3):61–86, 2002. In honour of Ronald C. Mullin.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma Algebra System I: The User Language. *J. Symbolic Comput.*, 24(3-4):235–265, October 1997.

[6] S. Bouyuklieva and I. Bouyukliev. An algorithm for classification of binary self-dual codes. *IEEE Trans. Inform. Theory*, 58(6):3933–3940, 2012.

[7] S. Bouyuklieva, A. Malevich, and W. Willems. Automorphisms of extremal self-dual codes. *IEEE Trans. Inform. Theory*, 56(5):2091–2096, 2010.

[8] S. Bouyuklieva and W. Willems. Singly even self-dual codes with minimal shadow. *IEEE Trans. Inform. Theory*, 58(6):3856–3860, 2012.

[9] S. Bouyuklieva, N. Yankov, and J. L. Kim. Classification of binary self-dual $[48, 24, 10]$ codes with an automorphism of odd prime order. *Finite Fields Appl.*, 18(6):1104–1113, 2012.

[10] S. Bouyuklieva, N. Yankov, and R. Russeva. Classification of the binary self-dual [42, 21, 8] codes having an automorphism of order 3. *Finite Fields Appl.*, 13(3):605–615, 2007.

[11] S. Bouyuklieva, N. Yankov, and R. Russeva. On the classication of binary self-dual [44, 22, 8] codes with an automorphism of order 3 or 7. *Int. J. Inf. Coding Theory*, 2(1):21–37, January 2011.

[12] S. Buyuklieva. On the binary self-dual codes with an automorphism of order 2. *Des. Codes Cryptogr.*, 12(1):39–48, 1997.

[13] J. H. Conway, V. Pless, and N. J. A. Sloane. The binary self-dual codes of length up to 32: a revised enumeration. *J. Combin. Theory Ser. A*, 60(2):183–195, 1992.

[14] J. H. Conway and N. J. A. Sloane. A new upper bound on the minimal distance of self-dual codes. *IEEE Trans. Inform. Theory*, 36(6):1319–1333, 1990.

[15] R. Dontcheva and M. Harada. Extremal doubly-even [80,40,16] codes with an automorphism of order 19. *Finite Fields Appl.*, 9(2):157–167, 2003.

[16] R. Dontcheva and V. Yorgov. The extremal codes of lengths 76 with an automorphism of order 19. *Finite Fields Appl.*, 9(4):395–399, 2003.

[17] R. A. Dontcheva, A. J. van Zanten, and S. M. Dodunekov. Binary self-dual codes with automorphisms of composite order. *IEEE Trans. Inform. Theory*, 50(2):311–318, 2004.

[18] S. T. Dougherty, T. A. Gulliver, and M. Harada. Extremal binary self-dual codes. *IEEE Trans. Inform. Theory*, 43(6):2036–2047, 1997.

[19] P. Gaborit and A Otmani. Tables of self-dual codes. Online available at http://www.unilim.fr/pages_perso/philippe.gaborit/SD/index.html.

[20] P. Gaborit and A. Otmani. Experimental constructions of self-dual codes. *Finite Fields Appl.*, 9(3):372–394, 2003.

[21] T. A. Gulliver and M. Harada. Classification of extremal double circulant self-dual codes of lengths 64 to 72. *Des. Codes Cryptogr.*, 13(3):257–269, 1998.

[22] T. A. Gulliver and M. Harada. Classification of extremal double circulant self-dual codes of lengths 74–88. *Discrete Math.*, 306(17):2064–2072, 2006.

[23] T. A. Gulliver, M. Harada, and J. L. Kim. Construction of new extremal self-dual codes. *Discrete Math.*, 263(1-3):81–91, 2003.

[24] M. Harada. The existence of a self-dual $[70, 35, 12]$ code and formally self-dual codes. *Finite Fields Appl.*, 3(2):131–139, 1997.

[25] M. Harada, T. A. Gulliver, and H. Kaneta. Classification of extremal double-circulant self-dual codes of length up to 62. *Discrete Math.*, 188(1-3):127–136, 1998.

[26] M. Harada and A. Munemasa. Database of self-dual codes. Online available at http://www.math.is.tohoku.ac.jp/~munemasa/selfdualcodes.htm.

[27] M. Harada and A. Munemasa. Some restrictions on weight enumerators of singly even self-dual codes. *IEEE Trans. Inform. Theory*, 52(3):1266–1269, 2006.

[28] M. Harada and A. Munemasa. Classification of self-dual codes of length 36. *Adv. Math. Commun.*, 6(2):229–235, 2012.

[29] W. C. Huffman. Automorphisms of codes with applications to extremal doubly even codes of length 48. *IEEE Trans. Inform. Theory*, 28(3):511–521, 1982.

[30] W. C. Huffman. On the classification and enumeration of self-dual codes. *Finite Fields Appl.*, 11(3):451–490, 2005.

[31] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[32] H. J. Kim. The binary extremal self-dual codes of lengths 38 and 40. *Des. Codes Cryptogr.*, 63(1):43–57, 2012.

[33] C. L. Mallows and N. J. A. Sloane. An upper bound for self-dual codes. *Inf. Control*, 22:188–200, 1973.

[34] V. Pless. A classification of self-orthogonal codes over GF(2). *Discrete Math.*, 3:209–246, 1972.

[35] V. Pless and N. J. A. Sloane. On the classification and enumeration of self-dual codes. *J. Combin. Theory Ser. A*, 18:313–335, 1975.

[36] E. M. Rains. Shadow bounds for self-dual codes. *IEEE Trans. Inform. Theory*, 44(1):134–139, 1998.

[37] E. M. Rains and N. J. A. Sloane. Self-dual codes. In *Handbook of coding theory, Vol. I, II*, pages 177–294. North-Holland, Amsterdam, 1998.

[38] D. K. Ray-Chaudhuri and R. M. Wilson. On t-designs. *Osaka J. Math.*, 12(3):737–744, 1975.

[39] N. Yankov. Self-dual [62, 31, 12] and [64, 32, 12] codes with an automorphism of order 7. *Adv. Math. Commun.*, 8(1):73–81, 2014.

[40] N. Yankov and M. H. Lee. Classification of self-dual codes of length 50 with an automorphism of odd prime order. *Des. Codes Cryptogr.*, 74(3):571–579, 2015.

[41] N. Yankov and M. H. Lee. New binary self-dual codes of lengths 50–60. *Des. Codes Cryptogr.*, 73(3):983–996, 2014.

[42] V. Yorgov. The extremal codes of length 42 with automorphism of order 7. *Discrete Math.*, 190(1-3):201–213, 1998.

[43] V. Y. Yorgov. Binary self-dual codes with automorphisms of odd order. *Problemy Peredachi Informatsii*, 19(4):11–24, 1983.

[44] V. Y. Yorgov. A method for constructing inequivalent self-dual codes with applications to length 56. *IEEE Trans. Inform. Theory*, 33(1):77–82, 1987.

[45] R. Yorgova and A. Wassermann. Binary self-dual codes with automorphisms of order 23. *Des. Codes Cryptogr.*, 48(2):155–164, 2008.