Classification of Self-Dual Codes of Length 36

Masaaki Harada*and Akihiro Munemasa†

March 21, 2012

Abstract

A complete classification of binary self-dual codes of length 36 is given.

Key words and phrases: self-dual code, weight enumerator, mass formula
2000 Mathematics Subject Classification: Primary: 94B05; Secondary: 94B75

1 Introduction

As described in [9], self-dual codes are an important class of linear codes for both theoretical and practical reasons. It is a fundamental problem to classify self-dual codes of modest lengths and much work has been done towards classifying self-dual codes over $\mathbb{F}_q$ for $q = 2$ and 3, where $\mathbb{F}_q$ denotes the finite field of order q and q is a prime power (see [9]).

Codes over $\mathbb{F}_2$ are called *binary* and all codes in this paper are binary unless otherwise noted. The *dual code* $C^\perp$ of a code C of length n is defined as $C^\perp = \{x \in \mathbb{F}_2^n \mid x \cdot y = 0 \text{ for all } y \in C\}$, where $x \cdot y$ is the standard inner product. A code C is called *self-orthogonal* if $C \subset C^\perp$, and C is called *self-dual* if $C = C^\perp$. A self-dual code C is *doubly even* if all codewords of C have weight divisible by four, and *singly even* if there is at least one codeword of weight $\equiv 2 \pmod 4$. It is known that a self-dual code of length n exists

*Department of Mathematical Sciences, Yamagata University, Yamagata 990–8560, Japan, and PRESTO, Japan Science and Technology Agency (JST), Kawaguchi, Saitama 332–0012, Japan. email: mharada@sci.kj.yamagata-u.ac.jp

†Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan. email: munemasa@math.is.tohoku.ac.jp

if and only if n is even, and a doubly even self-dual code of length n exists if and only if n is divisible by eight. Two codes are *equivalent* if one can be obtained from the other by permuting the coordinates. An *automorphism* of C is a permutation of the coordinates of C which preserves C. The set consisting of all automorphisms of C is called the *automorphism group* of C and it is denoted by $\mathrm{Aut}(C)$.

A classification of self-dual codes of lengths up to 30 and doubly even self-dual codes of length 32 is known (see [9, Table I]). A classification of singly even self-dual codes of length 32 is given in [3]. The classification is extended to length 34 [2]. Using the classification of self-dual codes of length 34 and minimum weight 6, extremal self-dual codes of length 36, that is, those with minimum weight 8, were classified in [8].

The main aim of this paper is to give a complete classification of self-dual codes of length 36, confirming in particular, the partial classification given in [8].

Theorem 1. *There are* 519492 *inequivalent self-dual codes of length* 36*. Of these* 41 *are extremal,* 58671 *have minimum weight* 6*,* 436633 *have minimum weight* 4*, and* 24147 *have minimum weight* 2*.*

Generator matrices of all inequivalent self-dual codes of length 36, as well as those of shorter lengths, can be obtained electronically from [6]. As a summary, we list in Table 1 the total number $\#_T$ of inequivalent self-dual codes of length n and the number $\#_d$ of inequivalent self-dual codes of length n and minimum weight d for $n = 2, 4, \ldots, 36$. All computer calculations in this paper were done by Magma [4].

2 Preliminaries

2.1 Classification method

Here we describe a method for classifying self-dual codes. This method is similar to that given in [7].

Suppose that C is a self-dual $[n, n/2, d]$ code with $d \geq 4$. Define a subcode of C as follows

$$C_0 = \{(x_1, x_2, \ldots, x_n) \in C \mid x_{n-1} = x_n\}.$$

Since $C^\perp$ has no codeword of weight 2, C_0 has dimension $n/2 - 1$. Permuting coordinates if necessary, we may assume that there is a codeword

Table 1: Numbers of self-dual codes

n	$\#_T$	$\#_2$	$\#_4$	n	$\#_T$	$\#_2$	$\#_4$	$\#_6$	$\#_8$
2	1	1	0	20	16	9	7	0	0
4	1	1	0	22	25	16	8	1	0
6	1	1	0	24	55	25	28	1	1
8	2	1	1	26	103	55	47	1	0
10	2	2	0	28	261	103	155	3	0
12	3	2	1	30	731	261	457	13	0
14	4	3	1	32	3295	731	2482	74	8
16	7	4	3	34	24147	3295	19914	938	0
18	9	7	2	36	519492	24147	436633	58671	41

$x = (x_1, \ldots, x_n)$ of weight d in C with $x_{n-1} = x_n \neq 0$. Then, the following code

$$C_1 = \{(x_1, x_2, \ldots, x_{n-2}) \mid (x_1, x_2, \ldots, x_n) \in C_0\}$$

is a self-dual $[n-2, n/2-1, d-2]$ code. Thus, the subcode C_0 has generator matrix of the form

$$G_0 = \left(\begin{array}{c|cc} & a_1 & a_1 \\ G_1 & \vdots & \vdots \\ & a_{n/2-1} & a_{n/2-1} \end{array} \right), \tag{1}$$

where G_1 is a generator matrix of C_1 and $a_i \in \mathbb{F}_2$ $(i = 1, \ldots, n/2-1)$. It follows that every self-dual $[n, n/2, d]$ code is constructed as the code $\langle C_0, x \rangle$ for some code C_0 with generator matrix of the form (1) and some vector $x \in C_0^{\perp} \setminus C_0$, where $\langle C_0, x \rangle$ denotes the code generated by the codewords of C_0 and x. Note that there is essentially a unique choice for $\langle C_0, x \rangle$, for a given C_0. Indeed, among the three self-dual codes lying between $C_0^{\perp}$ and C_0, two of them are equivalent, while the remaining code has minimum weight 2.

In this way, all self-dual $[n, n/2, d]$ codes D, which must be checked further for equivalence, are constructed, by taking generator matrices of all inequivalent self-dual $[n-2, n/2-1, d-2]$ codes D_1 as matrices G_1, and by considering $a_i \in \mathbb{F}_2$ $(i = 1, \ldots, n/2-1)$ in (1).

As described in [7], the number of possibilities for a_i $(i = 2, \ldots, n/2-1)$ is decreased by applying elements of $\mathrm{Aut}(D_1)$ to the first $n-2$ coordinates of D.

This can be made more precise and more general as follows. Two codes C and C' over $\mathbb{F}_q$ are monomially equivalent if there is some monomial matrix M over $\mathbb{F}_q$ such that $C' = CM = \{cM \mid c \in C\}$. The monomial automorphism group of C is the set of monomial matrices M with $C = CM$ and it is denoted by $\mathrm{MAut}(C)$. Let D_1 be a linear $[n, k]$ code over $\mathbb{F}_q$ with $k \times n$ generator matrix G_1. Then there exists a homomorphism $f : \mathrm{MAut}(D_1) \to \mathrm{GL}(k, q)$ defined by $f(P)G_1 = G_1P$, where $P \in \mathrm{MAut}(D_1)$. The image $\mathrm{Im}(f)$ is a subgroup of $\mathrm{GL}(k, q)$. With this notation, we have the following sufficient condition for monomial equivalence.

Lemma 2. *Let m be a positive integer, and let $a, b \in \mathbb{F}_q^k$. Suppose that a^T and b^T belong to the same $\mathrm{Im}(f)$-orbit (under the left action), where a^T denotes the transpose of a. Then the $[n + m, k]$ codes over $\mathbb{F}_q$ with generator matrices*

$$\begin{pmatrix} G_1 & a^T & \cdots & a^T \end{pmatrix} \text{ and } \begin{pmatrix} G_1 & b^T & \cdots & b^T \end{pmatrix}$$

are monomially equivalent.

Proof. There exists a monomial matrix $P \in \mathrm{MAut}(D_1)$ such that $a^T = f(P)b^T$. Then the monomial matrix

$$\begin{pmatrix} P & O \\ O^T & I_m \end{pmatrix}$$

gives a monomial equivalence of the two codes above, where I_m denotes the identity matrix of order m and O denotes the $n \times m$ zero matrix. □

In our case $(n, q) = (36, 2)$, we only need to consider $(a_1, \ldots, a_{17}) \in \mathbb{F}_2^{17}$ in (1), up to the action of $\mathrm{Im}(f)$ by Lemma 2. Orbit representatives for a subgroup of $\mathrm{GL}(17, 2)$ can easily be found by Magma [4].

2.2 Mass formula for weight enumerators

Now we give a mass formula for weight enumerators of self-dual codes.

Lemma 3 (Thompson [10])**.** *Let n be an even positive integer. Let $W_C(y)$ denote the weight enumerator of a code C. Then*

$$\sum_C W_C(y) = \Big(\prod_{i=1}^{n/2-1} (2^i + 1) \Big)(1 + y^n) + \sum_{j=1}^{n/2-1} \binom{n}{2j} \prod_{i=1}^{n/2-2} (2^i + 1) y^{2j}, \quad (2)$$

where C runs through the set of all self-dual codes of length n.

As a consequence, we have the following:

Lemma 4. *Let n and d be even positive integers. Let $\mathcal{C}$ be a family of inequivalent self-dual codes of length n and minimum weight at most d. Then $\mathcal{C}$ is a complete set of representatives for equivalence classes of self-dual codes of length n and minimum weight at most d, if and only if*

$$\sum_{C\in\mathcal{C}} \frac{n!}{\#\operatorname{Aut}(C)} \#\{x \in C \mid \operatorname{wt}(x) = d\} = \binom{n}{d} \prod_{i=1}^{n/2-2} (2^i + 1). \tag{3}$$

Proof. Consider the coefficient of y^d in the formula (2) in Lemma 3. □

3 Classification of self-dual codes of length 36

In this section, we give a complete classification of self-dual codes of length 36.

Any self-dual code of length $n+2$ and minimum weight 2 is decomposable as $i_2 \oplus C_n$, where i_2 is the unique self-dual code of length 2 and C_n is some self-dual code of length n. Since there are 24147 inequivalent self-dual codes of length 34 [2], there are 24147 inequivalent self-dual $[36, 18, 2]$ codes. We denote the set of these 24147 codes by $\mathcal{C}_{36,2}$.

For each self-dual $[34, 17, 2]$ code given in [2], the method given in Subsection 2.1 produces a number of self-dual $[36, 18, 4]$ codes. We continue the process until we obtain a set $\mathcal{C}_{36,4}$ of inequivalent self-dual $[36, 18, 4]$ codes such that $\mathcal{C} = \mathcal{C}_{36,2} \cup \mathcal{C}_{36,4}$ satisfies (3). Lemma 4 implies that there is no other self-dual $[36, 18, 4]$ code.

Similarly, we found the set $\mathcal{C}_{36,6}$ of the 58671 inequivalent self-dual $[36, 18, 6]$ codes from the set of inequivalent self-dual $[34, 17, 4]$ codes. Setting $\mathcal{C} = \mathcal{C}_{36,2} \cup \mathcal{C}_{36,4} \cup \mathcal{C}_{36,6}$ in Lemma 4, one can verify that there is no other self-dual $[36, 18, 6]$ code.

From our results, together with the set of extremal self-dual codes found by [8], we obtain the set $\mathcal{C}_{36}$ of 519492 inequivalent self-dual codes satisfying

$$\sum_{C\in\mathcal{C}_{36}} \frac{36!}{\#\operatorname{Aut}(C)} = \prod_{i=1}^{17} (2^i + 1),$$

which is the usual mass formula appearing as the constant term of (2). Since this constant term gives the number of distinct self-dual codes of length 36,

it follows that there is no other self-dual code of length 36. Therefore, we have Theorem 1.

4 Some properties

The weight enumerator of a self-dual code of length 36 can be written as

$$\begin{aligned}&1+\alpha y^2+(12\alpha+\beta)y^4+(64\alpha+6\beta+\gamma)y^6+(33+196\alpha+11\beta+64\delta)y^8\\&+(3168+364\alpha-4\beta-6\gamma-384\delta)y^{10}+(7059+364\alpha-39\beta+832\delta)y^{12}\\&+(30336-38\beta+15\gamma-512\delta)y^{14}+(58443-572\alpha+27\beta-896\delta)y^{16}\\&+(64064-858\alpha+72\beta-20\gamma+1792\delta)y^{18}+\cdots+y^{36},\end{aligned}$$

where $\alpha, \beta, \gamma, \delta$ are integers. The numbers of distinct weight enumerators of self-dual codes of length 36 are listed in Table 2 for each minimum weight d. In particular, we list in Table 3 the numbers of self-dual codes with $d = 6$ for each weight enumerator, where the numbers # of codes and (γ, δ) are listed.

Table 2: Numbers of weight enumerators

d	2	4	6	8
#	1264	2210	28	2

Table 3: Numbers of weight enumerators for $d = 6$

#	(γ, δ)	#	(γ, δ)	#	(γ, δ)	#	(γ, δ)
107	$(2, 3)$	257	$(8, 4)$	8493	$(16, 3)$	146	$(28, 3)$
41	$(2, 4)$	7710	$(10, 3)$	1	$(16, 4)$	122	$(30, 3)$
559	$(4, 3)$	183	$(10, 4)$	6432	$(18, 3)$	20	$(32, 3)$
111	$(4, 4)$	9739	$(12, 3)$	3773	$(20, 3)$	25	$(34, 3)$
1971	$(6, 3)$	82	$(12, 4)$	2319	$(22, 3)$	4	$(36, 3)$
214	$(6, 4)$	10262	$(14, 3)$	954	$(24, 3)$	5	$(38, 3)$
4535	$(8, 3)$	22	$(14, 4)$	579	$(26, 3)$	5	$(42, 3)$

The smallest order $\#\operatorname{Aut}_s$ and the largest order $\#\operatorname{Aut}_l$ among automorphism groups of self-dual codes of length 36 are listed in Table 4 for each

minimum weight d. In particular, for $d = 6$, the number N of the codes with an automorphism group of order $\#\,\mathrm{Aut}$ is listed in Table 5. There is no self-dual code with a trivial automorphism group for lengths up to 32 (see [3]). At length 34, there are 159 inequivalent self-dual $[34, 17, 6]$ codes with trivial automorphism groups. Compared to self-dual codes of length 34, there are a great number of self-dual codes with trivial automorphism groups for length 36.

Table 4: Orders of the automorphism groups

d	2	4	6	8
$\#\,\mathrm{Aut}_s$	2	4	1	6
$\#\,\mathrm{Aut}_l$	$2^{18} \cdot 18!$	$2^{17} \cdot 18!$	21504	34560

Table 5: Orders of the automorphism groups for $d = 6$

$\#\,\mathrm{Aut}$	N	$\#\,\mathrm{Aut}$	N	$\#\,\mathrm{Aut}$	N	$\#\,\mathrm{Aut}$	N	$\#\,\mathrm{Aut}$	N	$\#\,\mathrm{Aut}$	N
1	41019	14	1	56	1	192	25	576	2	3456	1
2	11242	16	643	64	118	240	3	768	12	4608	1
3	37	18	3	72	7	256	21	864	1	5376	1
4	3368	20	2	80	1	288	7	1152	4	5760	1
6	137	24	59	96	43	336	1	1344	1	12960	2
7	2	32	251	108	1	384	18	1536	5	21504	1
8	1297	36	21	128	45	432	1	1728	3		
12	166	48	78	144	9	512	8	2304	1		

Let C be a singly even self-dual code and let C_0 denote the subcode of codewords having weight $\equiv 0 \pmod 4$. Then C_0 is a subcode of codimension 1. The *shadow* S of C is defined to be $C_0^{\perp} \backslash C$. Let d and s denote the minimum weights of a self-dual code of length 36 and its shadow, respectively. It was shown in [1] that $2d + s \leq 22$. The numbers $\#_s$ of self-dual codes with shadows of minimum weight s are listed in Table 6 for each minimum weight d. Note that there is no self-dual $[36, 18, 4]$ code meeting the bound. A classification of self-dual $[36, 18, 6]$ codes meeting the bound can be found in [8].

The covering radius $R(C)$ of a code C is the smallest integer R such that spheres of radius R around codewords of C cover the space $\mathbb{F}_2^n$. The covering

Table 6: Minimum weights of the shadows

d	$\#_2$	$\#_6$	$\#_{10}$	$\#_{14}$	$\#_{18}$
2	679	22883	577	7	1
4	22541	414068	24	0	-
6	911	57755	5	-	-
8	16	25	-	-	-

radius is a basic and important geometric parameter of a code (see [5]). Let C be a self-dual $[36, 18, d]$ code. By [5, Eq. (2)] and the Delsarte bound (see [5, Theorem 2]),

$$6 \leq R(C) \leq 20 - d.$$

The numbers $\#R_r$ of self-dual codes of length 36 with covering radii r are listed in Table 7 for each minimum weight d. There is a unique self-dual $[36, 18, 6]$ code with covering radius 6. This code C_{36} has generator matrix $(\ I_{18}\ ,\ M\ )$ where M is listed in Figure 1. The code C_{36} has weight enumerator with $(\alpha, \beta, \gamma, \delta) = (0, 0, 12, 4)$, it has shadow of minimum weight 2 and it has automorphism group of order 5760.

Table 7: Covering radii of self-dual codes of length 36

d	$\#R_6$	$\#R_7$	$\#R_8$	$\#R_9$	$\#R_{10}$	$\#R_{11}$	$\#R_{12}$
2	0	23	20148	3010	830	87	34
4	23	372396	63599	587	28	0	0
6	1	53226	5439	0	5	0	0
8	3	38	0	0	0	0	0
d	$\#R_{13}$	$\#R_{14}$	$\#R_{15}$	$\#R_{16}$	$\#R_{17}$	$\#R_{18}$	
2	5	7	1	1	0	1	
4	0	0	0	0	-	-	
6	0	0	-	-	-	-	

We end this paper with some remark on the classification of self-dual codes of length 38. Since

$$\frac{\prod_{i=1}^{18}(2^i + 1)}{38!} > 13644432.203,$$

$$M = \begin{pmatrix} 001100000010100010 \\ 001100000010101101 \\ 000110000001110101 \\ 000110000001000110 \\ 001000000001100101 \\ 001000000010011001 \\ 101110001000111111 \\ 101110110111111100 \\ 110001000100100110 \\ 110010111011010110 \\ 010011011000110011 \\ 011100010111001111 \\ 001011100111000000 \\ 111011101000000011 \\ 010000101111100101 \\ 101111011111011010 \\ 110111110111101010 \\ 001011111011100110 \end{pmatrix}$$

Figure 1: A self-dual $[36, 18, 6]$ code with covering radius 6

there are at least 13644433 inequivalent self-dual codes of length 38.

Acknowledgment. This work of the first author was supported by JST PRESTO program.

References

[1] C. Bachoc and P. Gaborit, Designs and self-dual codes with long shadows, *J. Combin. Theory Ser. A* **105** (2004), 15–34.

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

[3] R.T. Bilous and G.H.J. van Rees, An enumeration of self-dual codes of length 32, *Des. Codes, Cryptogr.* **26** (2002), 61–86.

[4] W. Bosma and J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, Available online at `http://magma.maths.usyd.edu.au/magma/`.

[5] G.D. Cohen, M.G. Karpovsky, H.F. Mattson, Jr. and J.R. Schatz, Covering radius — Survey and recent results, *IEEE Trans. Inform. Theory* **31** (1985), 328–343.

[6] M. Harada and A. Munemasa, Database of Self-Dual Codes, Available online at `http://www.math.is.tohoku.ac.jp/~munemasa/selfdualcodes.htm`.

[7] W.C. Huffman, Characterization of quaternary extremal codes of lengths 18 and 20, *IEEE Trans. Inform. Theory* **43** (1997), 1613–1616.

[8] C.A. Melchor and P. Gaborit, On the classification of extremal binary self-dual codes, *IEEE Trans. Inform. Theory* **54** (2008), 4743–4750.

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

[10] J.G. Thompson, Weighted averages associated to some codes, *Scripta Math.* **29** (1973), 449–452.