Mathematica Balkanica

New Series Vol. 21, 2007, Fasc. 1-2

New Extremal Self-Dual Codes of Length 66

Masaaki Harada [1], *Takuji Nishimura* [1] *and Radinka Yorgova* [2]

Presented by P. Kenderov

A number of new extremal self-dual codes of length 66 having weight enumerators for which extremal self-dual codes were not previously known to exist, are constructed.

1. Introduction

A (binary) $[n, k]$ code C is a k-dimensional vector subspace of $\mathbb{F}_2^n$, where $\mathbb{F}_2$ is the field of two elements. An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d. A code C is *self-dual* if $C = C^\perp$ where $C^\perp$ is the dual code of C. 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 $\equiv 2 \pmod 4$. Note that a doubly-even self-dual code of length n exists if and only if n is divisible by eight. An automorphism of C is a permutation of the coordinates of C which preserves C. The set consisting of all automorphisms of C forms a group called the automorphism group of C.

A singly-even self-dual code is called *extremal* if it has the largest minimum weight among all singly-even self-dual codes of that length. Conway and Sloane [1] proved a new upper bound for the minimum weight of singly-even self-dual codes and gave a list of the possible weight enumerators of extremal singly-even self-dual codes for lengths $n \leq 64$ and length 72. Their work was extended to lengths up to 100 in [3]. Much work has been done concerning construction of extremal singly-even self-dual codes (see e.g., [1], [2], [3], [4], [8], [9], [10], [11], [14] and the references given therein). The largest minimum weight among self-dual code of length 66 is 12. The possible weight enumerators of extremal self-dual $[66, 33, 12]$ codes are

$$\begin{aligned} W_1 =& 1 + (858 + 8\alpha)y^{12} + (18678 - 24\alpha)y^{14} + \cdots \ (0 \le \alpha \le 778) \\ W_2 =& 1 + 1690y^{12} + 7990y^{14} + \cdots \\ W_3 =& 1 + (858 + 8\alpha)y^{12} + (18166 - 24\alpha)y^{14} + \cdots \ (14 \le \alpha \le 756), \end{aligned}$$

where α is a parameter [3]. An extremal self-dual code $D16$ in [1] has weight enumerator W_1 with $\alpha = 0$. It is shown in [4] that there are exactly three inequivalent double circulant self-dual $[66, 33, 12]$ codes. Two of these have weight enumerator W_1 with $\alpha = 0$, and the other has weight enumerator W_1 with $\alpha = 66$. Tsai [12] constructed two inequivalent extremal self-dual codes with weight enumerator W_2. The construction of extremal self-dual codes of length 66 is lacked comparing with the construction of the codes of lengths ≤ 64.

In this note, we construct a number of extremal self-dual $[66, 33, 12]$ codes with weight enumerators W_1 where $\alpha = 3, 8, 10, 14, 15, 16, 17, 22, 24, 26, 31, 36, 38, 41, 43, 45, 46, 52, 59, 73, 74, 76, 78, 80$, by several construction methods. These codes have weight enumerators for which extremal self-dual codes were not previously known to exist. A number of new extremal self-dual codes with weight enumerators W_2 are also constructed. The results in this note were already announced in the recent survey on self-dual codes written by Huffman [7].

2. Construction I

Let $G_0 = (\ I_n\ ,\ A\ )$ be a generator matrix of a self-dual code of length $2n$, where I_n denotes the identity matrix of order n. Let $(x_1, x_2, \ldots, x_n)$ be a vector of length n and odd (resp. even) weight if n is even (resp. odd). Then the following matrix

$$G = \begin{pmatrix} 1 & 0 & x_1 & \cdots & x_n & 1 & \cdots & 1 \\ y_1 & y_1 & & & & & & \\ \vdots & \vdots & & I_n & & & A & \\ y_n & y_n & & & & & & \end{pmatrix}$$

where $y_i = x_i + 1$ $(1 \le i \le n)$, generates a self-dual code C of length $2n + 2$ [5]. In this section, we construct new extremal self-dual codes of length 66 using this construction method.

A code having a generator matrix of the form $(\ I_n\ ,\ R\ )$ is called (pure) double circulant, where R is an $n \times n$ circulant matrix. It was shown in [4] that there exist exactly two extremal double circulant singly-even self-dual $[64, 32, 12]$ codes, up to equivalence. These codes have generator matrices M_1 and M_2 with the following first rows for R

$$(00010111110111000111111111100011) \text{ and}$$
$$(00000001000101001010011111000111),$$

respectively. Recently an extremal singly-even self-dual $[64, 32, 12]$ code has been found in [10]. A generator matrix of the form $(\ I \ , \ A \ )$ of the code is given in [10] and we denote the matrix A by M_3.

By the above method, from M_1, M_2 and M_3, we have found new extremal self-dual $[66, 33, 12]$ codes having weight enumerators for which extremal self-dual codes were not previously known to exist, where the results are listed in Table 1. In the table, we list the used generator matrices G_0, the vectors $x = (x_1, x_2, \ldots, x_{32})$, the weight enumerators W and the orders $|\mathrm{Aut}|$ of the automorphism groups for the new codes. The automorphism groups are calculated by Magma.

Table 1: New extremal self-dual $[66, 33, 12]$ codes I

Codes	G_0	Vectors x	W	$\|\mathrm{Aut}\|$
C_1	M_1	(11111010001000011000000010111000)	W_1 ($\alpha = 41$)	1
C_2	M_1	(11100010001000000000101001100000)	W_1 ($\alpha = 43$)	1
C_3	M_1	(11110001000000100000001100010110)	W_1 ($\alpha = 46$)	2
C_4	M_2	(11010110010110000000000000010000)	W_1 ($\alpha = 74$)	2
C_5	M_2	(11000011000010000010101000100000)	W_1 ($\alpha = 76$)	1
C_6	M_2	(11100100100001000100000000010100)	W_1 ($\alpha = 78$)	1
C_7	M_3	(10000010110000101010000100100101)	W_1 ($\alpha = 8$)	1
C_8	M_3	(10000101100010010100001010001100)	W_1 ($\alpha = 14$)	1
C_9	M_3	(00010000101001100100010001000010)	W_1 ($\alpha = 16$)	1
C_{10}	M_3	(00001000100100010010011000110000)	W_1 ($\alpha = 26$)	1

3. Construction II

In this section, we investigate extremal self-dual $[66, 33, 12]$ codes with an automorphism of order 7 using the technique developed by Huffman [6] and Yorgov [13]. Extremal singly-even self-dual codes of lengths $42, 50, 52, 54$ and $60, 64$ with automorphisms of order 7 have been investigated in [14], [8], [9], [11] and [2], respectively. In this section, we extend the work to length 66.

Suppose that σ is an automorphism of order 7 of an extremal self-dual $[66, 33, 12]$ code D. By [13, Theorem 1], one can show that σ consists of 9 7-cycles together with 3 fixed points. Let $E_\sigma(D)$ be the set of the vectors in D, which have even weight in each cycle of σ. Set $F_\sigma(D)$=$\{v \in D \mid v\sigma = v\}$. By

[6, Theorem 1], it follows $D = F_\sigma(D) \oplus E_\sigma(D)$ where $\oplus$ denotes the direct sum. Each vector v from $F_\sigma(D)$ is constant on any cycle of σ. Using the results from [2] we construct a possible generator matrix of the code D of the form:

$$G_{66} = \begin{pmatrix} & X & \\ Z & & O \end{pmatrix}, \tag{1}$$

where X is a 6×66 matrix generating the fixed subcode $F_\sigma(D)$ under σ of D and O is the 27×3 zero-matrix. Note that Z has the following form:

$$Z = \begin{pmatrix} r_0 & & & & & r_1 & r_2 & r_3 & r_4 \\ & r_0 & & & & r_5 & r_6 & r_7 & r_8 \\ & & r_0 & & & r_9 & r_{10} & r_{11} & r_{12} \\ & & & r_0 & & r_{13} & r_{14} & r_{15} & r_{16} \\ & & & & r_0 & r_{17} & r_{18} & r_{19} & r_{20} \\ k_1 & k_2 & k_3 & k_4 & k_5 & k_0 & & & \\ k_6 & k_7 & k_8 & k_9 & k_{10} & & k_0 & & \\ k_{11} & k_{12} & k_{13} & k_{14} & k_{15} & & & k_0 & \\ k_{16} & k_{17} & k_{18} & k_{19} & k_{20} & & & & k_0 \end{pmatrix},$$

where the cells r_i, k_i, for $i = 0, \dots, 20$, are 3×7 (right) circulant matrices with first rows corresponding to polynomials in $\mathbb{F}_2[x]/(x^7 - 1)$ and where the blanks are equal to the zero.

We have found many matrices of the form (1) which generate extremal self-dual $[66, 33, 12]$ codes. Here we present 11 codes D_i, $(i = 1, 2, \dots, 11)$, with weight enumerators for which extremal self-dual codes were not previously known to exist. For each code D_i, we denote the matrices X and Z in the generator matrices (1) by X_i and Z_i, respectively. In Tables 2 and 3, we give the matrices X_i and the cells of Z_i, respectively. In Table 2, a is the all-one vector of length 7 and the blanks are zero's, and in Table 3 u_i for $i = 0, \dots, 6$ and v_i for $i = 0, \dots, 6$, are 3×7 (right) circulant matrices with first rows 1110100, 0111010, 0011101, 1001110, 0100111, 1010011, 1101001, 1001011, 1100101, 1110010, 0111001, 1011100, 0101110 and 0010111 respectively, whereas the cell 0 denotes the 3×7 zero-matrix.

For the 11 codes D_i, we list the weight enumerators W and the orders $|\mathrm{Aut}|$ of the automorphism groups in Table 4. Note that an extremal self-dual code with weight enumerator W_1 $(\alpha = 66)$ is also found. Since the double circulant code with the same weight enumerator in [4] has no automorphism of order 7, the codes are inequivalent.

Table 2: Matrices X_i

X_1	a	a		a						0	1	0	X_7	a	a	a	a						0	0	0
	a	a	a							1	0	0				a	a	a					1	0	0
			a		a	a				1	0	0						a	a	a			1	0	0
					a	a	a			0	0	1							a	a	a		0	1	0
							a	a	a	0	0	1									a	a	0	1	1
		a				a			a	1	1	1			a		a			a		a	1	1	0
X_2	a	a	a							1	0	0	X_8	a	a	a	a						0	0	0
			a	a	a					1	0	0				a	a	a					1	0	0
				a	a	a				0	1	0						a	a	a			1	0	0
						a	a			0	1	1							a	a	a		0	1	0
							a	a	a	0	0	1									a	a	0	1	1
		a			a		a		a	1	1	0			a		a			a		a	1	1	0
X_3	a	a								1	1	0	X_9	a	a	a							1	0	0
		a	a	a						0	1	0			a	a	a						0	1	0
			a	a	a	a				0	0	0					a	a					0	1	1
					a	a	a	a		0	0	0						a	a	a			0	0	1
							a	a	a	0	0	1							a	a	a	a	0	0	0
				a		a		a	a	1	1	0				a				a		a	1	1	1
X_4	a	a	a							1	0	0	X_{10}	a	a	a							1	0	0
		a	a	a						0	1	0			a	a	a						0	1	0
				a	a	a				0	1	0					a	a					0	1	1
					a	a	a			0	0	1						a	a	a			0	0	1
							a	a	a	0	0	1							a	a	a	a	0	0	0
			a			a			a	1	1	1				a		a		a		a	1	1	0
X_5	a	a								1	1	0	X_{11}		a	a	a	a					0	0	0
		a	a	a						0	1	0		a		a	a						1	0	0
			a	a	a					0	0	1		a					a				1	1	0
					a	a	a			0	0	1							a	a			0	1	1
						a	a	a	a	0	0	0								a	a	a	0	0	1
				a			a		a	1	1	1		a	a		a			a		a	0	1	0
X_6	a	a	a	a						0	0	0													
			a	a	a	a				0	0	0													
					a	a	a			1	0	0													
							a	a		1	1	0													
								a	a	0	1	1													
		a		a		a				1	1	1													

4. Construction III

Two self-dual codes C and C' of length n are called *neighbors* if the dimension of $C \cap C'$ is $n/2 - 1$. Let $v \in \mathbb{F}_2^{66}$ be a vector of even weight and let C be a self-dual code of length 66. For v and C ($v \notin C$), we define $N(v, C)$ as follows:

$$N(v, C) = (C \cap \langle v \rangle^{\perp}) \cup \{u + v \mid u \in (C \cap \langle v \rangle^{\perp})\}.$$

Then it is well known that $N(v, C)$ is a self-dual code which is a neighbor of C.

As described in Section 1,the code $D16$ in [1] is an extremal self-dual double circulant code with generator matrix (I_{33} , R) where R is the circulant matrix with first row

(00000101100101101100101111011001).

Using the above neighbor construction, we have found new extremal self-dual codes having weight enumerators for which extremal self-dual codes were not previously known to exist. For the new self-dual neighbors $N(C, v)$, C, v, the weight enumerators W and the orders $|\mathrm{Aut}|$ of the automorphism groups are

Table 3: Cells of the matrices Z_i

Codes	$r_0, r_1, \dots, r_{20}, k_0, k_1, \dots, k_{20}$
D_1	$u_0,u_0,u_0,u_0,u_0,u_0,u_1,u_1,u_1,u_0,u_1,u_1,u_2,u_0,u_1,u_2,u_2,u_0,u_5,u_2,u_4$ $v_0,v_0,v_0,v_0,v_0,v_0,v_0,v_1,v_1,v_1,v_5,v_0,v_1,v_1,v_2,v_2,v_0,v_1,v_2,v_2,v_4$
D_2	$u_0,u_0,u_0,u_0,u_0,u_0,0,0,u_0,u_0,0,0,u_1,u_0,0,u_0,u_3,u_0,u_5,u_2,u_1$ $v_0,v_0,v_0,v_0,v_0,v_0,v_0,0,0,0,v_5,v_0,0,0,v_0,v_2,v_0,v_0,v_1,v_3,v_1$
D_3	$u_0,u_0,u_0,u_0,u_0,u_0,0,0,u_0,u_0,0,0,u_1,u_0,0,u_0,u_3,u_0,u_0,u_6,u_5$ $v_0,v_0,v_0,v_0,v_0,v_0,v_0,0,0,0,v_0,v_0,0,0,v_0,v_6,v_0,v_0,v_1,v_3,v_5$
D_4	$u_0,u_0,u_0,u_0,u_0,u_0,0,0,u_0,u_0,0,0,u_1,u_0,0,u_0,u_2,u_0,u_2,u_3,u_2$ $v_0,v_0,v_0,v_0,v_0,v_0,v_0,0,0,0,v_2,v_0,0,0,v_0,v_3,v_0,v_0,v_1,v_2,v_2$
D_5	$u_0,u_0,u_0,u_0,u_0,u_0,0,0,u_0,u_0,0,0,u_1,u_0,0,u_0,u_2,u_0,u_3,u_0,u_3$ $v_0,v_0,v_0,v_0,v_0,v_0,v_0,0,0,0,v_3,v_0,0,0,v_0,v_0,v_0,v_0,v_1,v_2,v_3$
D_6	$u_0,u_0,u_0,u_0,u_0,u_0,0,0,u_0,u_0,0,0,u_1,u_0,0,u_0,u_2,u_0,u_1,u_2,u_3$ $v_0,v_0,v_0,v_0,v_0,v_0,v_0,0,0,0,v_1,v_0,0,0,v_0,v_2,v_0,v_0,v_1,v_2,v_3$
D_7	$u_0,u_0,u_0,u_0,u_0,u_0,0,0,u_0,u_0,0,0,u_1,u_0,0,u_0,u_2,u_0,u_1,u_5,u_3$ $v_0,v_0,v_0,v_0,v_0,v_0,v_0,0,0,0,v_1,v_0,0,0,v_0,v_5,v_0,v_0,v_1,v_2,v_3$
D_8	$u_0,u_0,u_0,u_0,u_0,u_0,0,0,u_0,u_0,0,0,u_1,u_0,0,u_0,u_2,u_0,u_2,u_5,0$ $v_0,v_0,v_0,v_0,v_0,v_0,v_0,0,0,0,v_2,v_0,0,0,v_0,v_5,v_0,v_0,v_1,v_2,0$
D_9	$u_0,u_0,u_0,u_0,u_0,u_0,0,0,u_0,u_0,0,0,u_1,u_0,0,u_0,u_2,u_0,u_3,u_2,u_6$ $v_0,v_0,v_0,v_0,v_0,v_0,v_0,0,0,0,v_3,v_0,0,0,v_0,v_2,v_0,v_0,v_1,v_2,v_6$
D_{10}	$u_0,u_0,u_0,u_0,u_0,u_0,0,0,u_0,u_0,0,0,u_1,u_0,0,u_0,u_4,u_0,u_1,0,u_2$ $v_0,v_0,v_0,v_0,v_0,v_0,v_0,0,0,0,v_1,v_0,0,0,v_0,0,v_0,v_0,v_1,v_4,v_2$
D_{11}	$u_0,u_0,u_0,u_0,u_0,u_0,u_1,u_1,u_1,u_0,u_1,u_1,u_2,u_0,u_1,u_2,u_3,u_0,u_1,u_2,u_5$ $v_0,v_0,v_0,v_0,v_0,v_0,v_0,v_1,v_1,v_1,v_1,v_0,v_1,v_1,v_2,v_2,v_0,v_1,v_2,v_3,v_5$

listed in Table 5 where

$$v_1 = (111101111111111011111111110111111 \quad 000000000000000000000000000000000)$$

$$v_2 = (100100000100000000100001000000100 \quad 100101111101101111101111111111101)$$

$$v_3 = (000000000000000000000000000000000 \quad 011011100010110111000101101110001).$$

Table 4: New extremal self-dual $[66, 33, 12]$ codes II

Codes	W	$\|\mathrm{Aut}\|$	Codes	W	$\|\mathrm{Aut}\|$
D_1	W_1 ($\alpha = 3$)	7	D_2	W_1 ($\alpha = 10$)	7
D_3	W_1 ($\alpha = 17$)	7	D_4	W_1 ($\alpha = 24$)	7
D_5	W_1 ($\alpha = 31$)	7	D_6	W_1 ($\alpha = 38$)	7
D_7	W_1 ($\alpha = 45$)	7	D_8	W_1 ($\alpha = 52$)	7
D_9	W_1 ($\alpha = 59$)	7	D_{10}	W_1 ($\alpha = 73$)	7
D_{11}	W_1 ($\alpha = 80$)	7			

Table 5: New extremal self-dual $[66, 33, 12]$ codes III

Codes	C	v	W	$\lvert\mathrm{Aut}\rvert$
E_1	$D16$	v_1	W_1 ($\alpha = 15$)	15
E_2	$C_{66,25}$ in [4]	v_2	W_1 ($\alpha = 22$)	220
E_3	$C_{66,25}$ in [4]	v_3	W_1 ($\alpha = 36$)	60

As described in Section , Tsai [12] constructed two codes with the weight enumerator W_2. The two codes are denoted by T66 and T66′ in [12]. We remark that both T66 and T66′ are neighbors of $D16$. In fact, if

$$v = (110101101110001000111011000001111 \\ 111101010111111100011010010010011)$$

then we find $\mathrm{T66} = N(D16, v)$.

Table 6: Extremal self-dual $[66, 33, 12]$ codes with weight enumerator W_2

41024713577, 41024737517, 41034175676, 41034512156, 41067152331, 41067174071
41067573512, 41076335057, 41124157354, 41125151432, 41125556333, 45476332745
45663336673, 45732732567, 46427334742, 46433352450, 46433754565, 46436310766
46476332475, 47473730744, 47522336751, 47536312452, 47736710561, 47737731462
54426371640, 54476713763, 61136775505, 61177060726, 61327061524, 61377243367
61537742727, 61727342776, 61736554744, 61767444306, 63126252505, 63126741144
63166570374, 63176256337, 63177564356, 63536172756, 63566661714, 63566670155
63567652115, 63726274537, 63776467126, 65126377115, 65126574146, 65136142154
65137042327, 65137142127, 65336067714, 65337744347, 65366144507, 65377554127
65532332757, 65536546564, 65572374550, 65732332455, 65732716644, 65736354544
65736455704, 65766544744, 66562730655, 67136771526, 67166254146, 67167574316
67177342137, 67526357441, 71137264374, 71166364107, 71326250556, 71337344357
71526752567, 71527353566, 71537541727, 73127741727, 73176466726, 73326052575
73326450575, 73527072554, 73537062554, 74723310646, 74762333451, 75166065306
75177041104, 75326367516, 75366045104, 75567061106, 75727253147, 76532713454
77136075347, 77166052745, 77366471575, 77377066126, 77526333466, 77526752507
77563375474, 77726166156, 77766045505, 77767156736

Moreover, we have found a number of new extremal self-dual codes $N(\mathrm{T66}, v)$ with the weight enumerator W_2 as self-dual neighbors of T66 under the assumption that v has the form $(v_1, v_2, \dots, v_{33}, 0, \dots, 0)$. In Table 6, we give the vectors $(v_1, v_2, \dots, v_{33})$ for 100 self-dual neighbors where the vectors $(v_1, v_2, \dots, v_{33})$ are written in octal using $0 = (000)$, $1 = (001), \dots,$ $6 = (110)$

and 7 = (111) to save space. Using Magma, we have verified that the 100 codes are inequivalent and have a trivial automorphism group. Since we have verified that the codes T66 and T66′ have an automorphism group of order 5, our codes are inequivalent to the two codes.

References

[1] 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** (1990), 1319–1333.

[2] R. Dontcheva and M. Harada, Some extremal self-dual codes with an automorphism of order 7, *Appl. Alge. Eng. Comm. Comput.* **14** (2003), 75–79.

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

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

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

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

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

[8] W.C. Huffman and V.D. Tonchev, The existence of extremal self-dual $[50, 25, 10]$ codes and quasi-symmetric 2-$(49, 9, 6)$ designs, *Designs, Codes and Cryptogr.* **6** (1996), 97–106.

[9] W.C. Huffman and V.D. Tonchev, The $[52, 26, 10]$ binary self-dual codes with an automorphism of order 7, *Finite Fields and Their Appl.* **7** (2001), 341–349.

[10] T. Nishimura, A new extremal self-dual code of length 64, *IEEE Trans. Inform. Theory* **50** (2004), 2173–2174.

[11] V.D. Tonchev and V.Y. Yorgov, The existence of certain extremal [54, 27, 10] self-dual codes, *IEEE Trans. Inform. Theory* **42** (1996), 1628–1631.

[12] H.-P. Tsai, Extremal self-dual codes of lengths 66 and 68, *IEEE Trans. Inform. Theory* **45** (1999), 2129–2133.

[13] V.Y. Yorgov, Binary self-dual codes with automorphisms of odd order, (Russian), *Probl. Perda. Inform.* **19** (1983), 11–24. English translation in *Probl. Inform. Transm.* **19** (1983), 260–270.

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

[1] *Department of Mathematical Sciences,*
Yamagata University,
Yamagata 990–8560, JAPAN

Received 12.12.2005

[2] *Department of Informatics,*
University of Bergen,
Thormøhlensgate 55,
N-5008, Bergen, NORWAY