New Binary Singly Even Self-Dual Codes

Masaaki Harada[*], Michael Kiermaier[†], Alfred Wassermann[‡] and Radinka Yorgova[§]

October 21, 2009

Abstract

In this correspondence, we construct new binary singly even self-dual codes with larger minimum weights than the previously known singly even self-dual codes for several lengths. Several known construction methods are used to construct the new self-dual codes.

1 Introduction

As described in [21], 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 length and determine the largest minimum weight among self-dual codes of that length. By the Gleason–Pierce theorem, there are nontrivial divisible self-dual codes over $\mathbb{F}_q$ for $q = 2, 3$ and 4 only, where $\mathbb{F}_q$ denotes the finite field of order q, and this is one of the reason why much work has been done concerning self-dual codes over these fields.

A code over $\mathbb{F}_2$ is called binary and all codes in this correspondence are binary. 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*

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

[†]Department of Mathematics, University of Bayreuth, D-95440 Bayreuth, Germany

[‡]Department of Mathematics, University of Bayreuth, D-95440 Bayreuth, Germany

[§]Department of Informatics, University of Bergen, Thormøhlensgate 55, N-5008, Bergen, Norway

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. It was shown in [19] that the minimum weight d of a doubly even self-dual code of length n is bounded by $d \leq 4[n/24]+4$. In [20] it is proved that the same bound is valid also for the minimum weight d of a singly even self-dual code of length n unless $n \equiv 22 \pmod{24}$ when $d \leq 4[n/24]+6$ or $n \equiv 0 \pmod{24}$ when $d \leq 4[n/24]+2$. The current state of knowledge about the largest minimum weight $d(n)$ among singly even self-dual codes of length n can be found in [8, Table VI] and [10, Table 2] for lengths $n \leq 130$.

In this correspondence, we construct new singly even self-dual codes with larger minimum weights than the previously known singly even self-dual codes for lengths $94, 98, 104, 122, 124, 128$ and 130. Several known construction methods are used to construct the new self-dual codes.

As a summary, we list bounds on $d(n)$ in Table 1 for $72 \leq n \leq 130$, which updates [8, Table VI] and [10, Table 2]. We list references which indicate the first self-dual code with the largest minimum weight among currently known self-dual codes of that length. For lengths $122, 124$ and 126, the upper bounds on the minimum weights have been improved by Han and Lee [13].

Table 1: Largest minimum weights of singly even self-dual codes

n	$d(n)$	Codes	n	$d(n)$	Codes	n	$d(n)$	Codes
72	12, 14	[5]	96	16, 18	[10]	120	18, 20, 22	[10]
74	12, 14	[5]	98	16, 18	C_{98}	122	20, 22	C_{122}
76	14	[1]	100	16, 18	[10]	124	20, 22	C_{124}
78	14	[5]	102	18	[10]	126	18, 20, 22	[10]
80	14, 16	[5]	104	18, 20	$N_{QR_{104}}(v)$	128	20, 22, 24	C_{128}
82	14, 16	[8]	106	16, 18	[23]	130	20, 22, 24	C_{130}
84	14, 16	[8]	108	16, 18, 20	[10]			
86	16	[8]	110	18, 20	[14]			
88	16	[16]	112	18, 20	[14]			
90	14, 16	[8]	114	18, 20	[10]			
92	16	[11]	116	18, 20	[10]			
94	16, 18	C_{94}	118	18, 20, 22	[10]			

2 A self-dual [94, 47, 16] code

An extremal doubly even self-dual $[24k, 12k, 4k+4]$ code is known for only $k = 1, 2$, namely, the extended Golay $[24, 12, 8]$ code and the extended quadratic residue $[48, 24, 12]$ code. It is not known if there exist other extremal doubly even self-dual codes of length $24k$. It was shown in [20] that the existences of an extremal doubly even self-dual $[24k, 12k, 4k + 4]$ code and a self-dual $[24k-2, 12k-1, 4k+2]$ code are equivalent. From this viewpoint, it would be interesting to determine the largest minimum weight among self-dual codes of length $24k - 2$. The largest minimum weight among self-dual codes of length 70 is known as 12 or 14, and the largest minimum weight among self-dual codes of length 94 was previously known as $14, 16$ or 18 (see [8, Table VI], [10, Table 2]). In this section, we give the first example of a self-dual $[94, 47, 16]$ code.

An automorphism of a code C is a permutation of the coordinates of C which preserves C and the set consisting of all automorphisms of C forms a group called the automorphism group of C. Self-dual codes with automorphisms of a fixed odd prime order have been widely investigated (see e.g., [17] and [22]). Using the technique developed in [17] and [22], we have found a self-dual $[94, 47, 16]$ code C_{94} with an automorphism of order 23. The code C_{94} has the following generator matrix:

$$
\left(\begin{array}{cccc|cc}
\boldsymbol{a} & & \boldsymbol{a} & & & \\
 & \boldsymbol{a} & & & 1 & \\
 & & & \boldsymbol{a} & & 1 \\
\hline
E_1 & & E_2 & E_2 & & \\
 & E_1 & E_3 & E_4 & & \\
F_2 & F_3 & F_1 & & & \\
F_2 & F_4 & & F_1 & &
\end{array}\right),
$$

where $\boldsymbol{a}$ is the all-one's vector of length 23, E_i $(i = 1, 2, 3, 4)$ and F_j $(j = 1, 2, 3, 4)$ are the 11×23 circulant matrices M with first rows r as follows:

M	r	M	r
E_1	(10000101001100110101111)	F_1	(11111010110011001010000)
E_2	(11010001001111110100100)	F_2	(10010010111111001000101)
E_3	(10001110110000111010101)	F_3	(11010101110000110111000)
E_4	(10001000010001010011100)	F_4	(10011100101000100001000)

and the blanks are filled up with zero's. Hence we have the following:

Proposition 1. *There is a self-dual* $[94, 47, 16]$ *code. The largest minimum weight among self-dual codes of length* 94 *is* 16 *or* 18.

We have verified by MAGMA [2] that C_{94} has automorphism group of order 23. Recall that two self-dual codes C and C' of length n are said to be *neighbors* if $\dim(C \cap C') = n/2 - 1$. Using observations on self-dual codes constructed by neighbors given in [4], we have verified that C_{94} has no self-dual $[94, 47, 18]$ neighbor.

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 $C_0^\perp \setminus C$ [5]. There are cosets C_1, C_2, C_3 of C_0 such that $C_0^\perp = C_0 \cup C_1 \cup C_2 \cup C_3$ where $C = C_0 \cup C_2$ and $S = C_1 \cup C_3$. Shadows are often used to provide restrictions on the weight enumerators of singly even self-dual codes. By 4) in [5, Theorem 5], a self-dual $[94, 47, 16]$ code C and its shadow S have the following possible weight enumerators:

$$\begin{aligned}
W_C =& 1 + 2\alpha y^{16} + (134044 - 2\alpha + 128\beta)y^{18} \\
&+ (2010660 - 30\alpha - 896\beta + 8192\gamma)y^{20} \\
&+ (22385348 + 30\alpha + 1280\beta - 106496\gamma - 524288\delta)y^{22} + \cdots, \\
W_S =& \delta y^3 + (\gamma - 22\delta)y^7 + (-\beta - 20\gamma + 231\delta)y^{11} \\
&+ (\alpha + 18\beta + 190\gamma - 1540\delta)y^{15} + \cdots,
\end{aligned}$$

respectively, where $\alpha, \beta, \gamma, \delta$ are integers. By 3) in [5, Theorem 5], we have the restrictions $(\delta, \gamma) = (0, 0), (0, 1), (1, 22)$. In the case $(\delta, \gamma) = (1, 22)$, we have $\beta = -209$ since the sum of two vectors in the shadow is a codeword. To save space, we do not list the possible weight enumerators for each of the three cases.

By verifying that the number of codewords of weight 16 in C_{94} is 6072 and that the minimum weight of the shadow is 15, the weight enumerators of C_{94} and its shadow are determined as follows:

$$1 + 6072y^{16} + 127972y^{18} + 1919580y^{20} + 22476428y^{22} + 207945348y^{24} + 1544755716y^{26} + 9310480316y^{28} + 45912129029y^{30} + 186607647954y^{32} + 629006183988y^{34} + 1767212902156y^{36} + 4155346712556y^{38} + 8204140462980y^{40} + 13635441761172y^{42} + 19112684048172y^{44} + 22621304618224y^{46} + \cdots,$$

$$3036y^{15} + 1023776y^{19} + 140516064y^{23} + 7782503008y^{27} + 189566779792y^{31} + 2156607786528y^{35} + 11933275327008y^{39} + 32978781634656y^{43} + 46205177207592y^{47} + \cdots,$$

respectively. Hence the weight enumerator of the code C_{94} corresponds to $(\alpha, \beta, \gamma, \delta) = (3036, 0, 0, 0)$. Since the code C_{94} has shadow of minimum weight 15, a doubly even self-dual $[96, 48, 16]$ code C_{96} can be constructed by Theorem 1 in [3]. We note that it has the largest minimum weight among known doubly even self-dual codes of length 96. Moreover, from the construction and the weight enumerators of C_{94} and its shadow, C_{96} has the following weight enumerator:

$$1 + 9108y^{16} + 3071328y^{20} + 370937840y^{24} + 18637739040y^{28} + \cdots.$$

Hence C_{96} and the codes in [7], [8] and [9] have different weight enumerators.

3 A self-dual [98, 49, 16] code

The largest minimum weight among self-dual codes of length 98 was previously known as $14, 16$ or 18 (see [10, Table 2]). Self-dual codes with automorphisms of odd composite order have been investigated (see e.g., [6] and [24]). Using the technique developed in [6] and [24], we have found a self-dual $[98, 49, 16]$ code C_{98} with an automorphism of order 15 with six 15-cycles, two 3-cycles and two fixed points.

A generator matrix G_{98} of the code C_{98} is given in Figure 1, where $\boldsymbol{a}$ is the all-one's vector of length 15, $\boldsymbol{b}$ is the all-one's vector of length 3, V_i $(i = 1, \dots, 8)$, S_j $(j = 1, 2, 3)$ and P_t $(t = 1, 2, 3)$ are 4×15 circulant matrices, L_k $(k = 1, 2, 3)$ are 2×15 circulant matrices whereas E is the 2×3 circulant matrix with first row (011) and the blanks are filled up with zero's. The first rows r of these circulant matrices V_i, S_j, P_t and L_k are listed in Table 2. Hence we have the following:

$$
G_{98} = \left(\begin{array}{cccccc|cc|cc}
\boldsymbol{a} & & & & & & & \boldsymbol{b} & 1 & 1 \\
& \boldsymbol{a} & & & & & \boldsymbol{b} & & 1 & 1 \\
& & \boldsymbol{a} & & & & \boldsymbol{b} & \boldsymbol{b} & & 1 \\
& & & & \boldsymbol{a} & & \boldsymbol{b} & \boldsymbol{b} & 1 & \\
& & & \boldsymbol{a} & & \boldsymbol{a} & & & & \\
\hline
V_1 & & & & V_2 & V_3 & & & & \\
& V_1 & & V_2 & V_4 & V_5 & & & & \\
& & V_1 & V_6 & V_7 & V_8 & & & & \\
S_1 & & & & S_2 & S_3 & & & & \\
& S_1 & & & S_3 & S_2 & & & & \\
& & S_1 & & S_3 & S_2 & & & & \\
& & & S_1 & S_3 & S_2 & & & & \\
P_2 & P_3 & P_3 & P_3 & P_1 & & & & & \\
P_3 & P_2 & P_2 & P_2 & & P_1 & & & & \\
& & & L_2 & L_2 & L_3 & E & & & \\
& & L_2 & L_2 & & L_3 & & E & & \\
L_1 & & L_1 & L_1 & L_1 & & & & & \\
& L_1 & L_2 & & L_2 & L_3 & & & &
\end{array}\right)
$$

Figure 1: A generator matrix G_{98} of C_{98}

Proposition 2. *There is a self-dual* $[98, 49, 16]$ *code. The largest minimum weight among self-dual codes of length* 98 *is* 16 *or* 18.

We have verified by MAGMA [2] that C_{98} has automorphism group of order 15. Using observations on self-dual codes constructed by neighbors given in [4], we have verified that C_{98} has no self-dual $[98, 49, 18]$ neighbor.

Table 2: First rows r of circulant matrices in G_{98}

	r		r		r
V_1	(011110111101111)	V_7	(011110111101111)	P_2	(111010110010001)
V_2	(110001100011000)	V_8	(001010010100101)	P_3	(101100100011110)
V_3	(101001010010100)	S_1	(000100110101111)	L_1	(011011011011011)
V_4	(011000110001100)	S_2	(110001001101011)	L_2	(011011011011011)
V_5	(110111101111011)	S_3	(101111000100110)	L_3	(110110110110110)
V_6	(100101001010010)	P_1	(011110101100100)		

By 4) in [5, Theorem 5], a self-dual $[98, 49, 16]$ code C and its shadow S

have the following possible weight enumerators:

$$\begin{aligned}
W_C =& 1 + (-13965 + \varepsilon)y^{16} + (56791 + 32\delta + \varepsilon)y^{18}\\
&+ (1480192 + 2048\gamma - 160\delta - 16\varepsilon)y^{20}\\
&+ (16081408 + 131072\beta - 22528\gamma - 96\delta - 16\varepsilon)y^{22}\\
&+ (161249200 + 8388608\alpha - 2228224\beta + 94208\gamma + 1760\delta + 120\varepsilon)y^{24} + \cdots,\\
W_S =& \alpha y + (-24\alpha - \beta)y^5 + (276\alpha + 22\beta + \gamma)y^9\\
&+ (-2024\alpha - 231\beta - 20\gamma - \delta)y^{13}\\
&+ (10626\alpha + 1540\beta + 190\gamma + 18\delta + 2\varepsilon)y^{17} + \cdots,
\end{aligned}$$

respectively, where $\alpha, \beta, \gamma, \delta, \varepsilon$ are integers. By 3) in [5, Theorem 5], we have the restrictions on α, β, γ as follows: $(\alpha, \beta) = (0, 0)$ or $(\alpha, \beta, \gamma) = (0, -1, 22), (1, -24, 252)$.

By verifying that the number of codewords of weights 16 and 18 in C_{98} are 4098 and 71782, respectively, and that the minimum weight of the shadow is 13, the weight enumerators of C_{98} and its shadow are determined as follows:

$$\begin{aligned}
&1 + 4098y^{16} + 71782y^{18} + 1206544y^{20} + 15801616y^{22} + 163247800y^{24}\\
&+ 1356343448y^{26} + 9169891120y^{28} + 50909529904y^{30} + 233822409070y^{32}\\
&+ 894025332265y^{34} + 2860857400336y^{36} + 7695423884304y^{38}\\
&+ 17462739820776y^{40} + 33526024003656y^{42} + 54577179576240y^{44}\\
&+ 75458884768688y^{46} + 88704403419008y^{48} + \cdots,\\
&96y^{13} + 34398y^{17} + 9002368y^{21} + 966180880y^{25} + 44270042080y^{29}\\
&+ 935282043976y^{33} + 9587762349984y^{37} + 49406723532912y^{41}\\
&+ 130985313214112y^{45} + 181029300619700y^{49} + \cdots,
\end{aligned}$$

respectively. Hence the weight enumerator of the code C_{98} corresponds to $(\alpha, \beta, \gamma, \delta, \varepsilon) = (0, 0, 0, -96, 18063)$.

4 Self-dual [104, 52, 18] codes

The largest minimum weight among singly even self-dual codes of length 104 was previously known as 16, 18 or 20 (see [10, Table 2]). In this section, we construct singly even self-dual $[104, 52, 18]$ codes. To do this, we need the following lemma. The construction method given in the lemma was used in [3] to construct an extremal singly even self-dual $[48, 24, 10]$ code whose shadow has minimum weight 4. We give a proof of this lemma for completeness.

Lemma 3. *Let C be a doubly even self-dual $[8n, 4n, d]$ code with $d \geq 8$. Let $v \in \mathbb{F}_2^{8n}$ be a vector of weight 4. Then*

$$N_C(v) = (C \cap \langle v \rangle^\perp) \cup \{u + v \mid u \in (C \setminus (C \cap \langle v \rangle^\perp))\}$$

is a singly even self-dual neighbor of C whose shadow is $(C \setminus (C \cap \langle v \rangle^\perp)) \cup \{u + v \mid u \in (C \cap \langle v \rangle^\perp)\}$. Moreover, $N_C(v)$ has minimum weight $\geq d - 2$ and its shadow has minimum weight 4.

Proof. It follows from Lemma 3 in [3] that $N_C(v)$ is a singly even self-dual neighbor and the shadow is $(C \setminus (C \cap \langle v \rangle^\perp)) \cup \{u + v \mid u \in (C \cap \langle v \rangle^\perp)\}$. Note that $(C \cap \langle v \rangle^\perp)$ is a subcode of C of index 2 and $(C \cap \langle v \rangle^\perp)$ has minimum weight $\geq d$. Let u be a codeword of weight d in C such that v and u are not orthogonal. Since the cardinality of the intersections of v and u is 1 or 3, we have $\mathrm{wt}(u+v) = d+2$ or $d-2$, respectively. Hence $\{u+v \mid u \in (C \setminus C \cap \langle v \rangle^\perp)\}$ has minimum weight $\geq d - 2$. Since the shadow contains the vector v, the minimum weight of the shadow is 4. □

Remark 4. If the cardinality of the intersections of v and u is 1 for all codewords u of minimum weight, then $N_C(v)$ has minimum weight $\geq d$.

The extended quadratic residue code QR_{104} of length 104 is an extremal doubly even self-dual code, i.e., its minimum weight is 20. Let $v \in \mathbb{F}_2^{104}$ be a vector of weight 4. By Lemma 3, $N_{QR_{104}}(v)$ is a singly even self-dual neighbor of QR_{104} and has minimum weight 18 or 20.

Let $M = (m_{ij})$ be the 1138150×104 matrix with rows composed of the codewords of weight 20 in QR_{104}. Let $\{j_1, j_2, j_3, j_4\}$ be the support of v. Define n_3 as the number of rows r such that $\mathrm{wt}(m_{rj_1}, m_{rj_2}, m_{rj_3}, m_{rj_4}) = 3$. We have verified that n_3 is positive for any set of distinct j_1, j_2, j_3, j_4. For a vector $v \in \mathbb{F}_2^{104}$ of weight 4, the singly even self-dual neighbor $N_{QR_{104}}(v)$ has minimum weight 18, since the number of codewords of weight 18 in $N_{QR_{104}}(v)$ is given by n_3.

Let C be a singly even self-dual $[104, 52, 18]$ code whose shadow S has minimum weight 4. By 4) in [5, Theorem 5], C and S have the following possible weight enumerators:

$$\begin{aligned}W_C =&1 + (34580 + 4\alpha)y^{18} + (620990 - 8\alpha)y^{20} + (7570900 - 60\alpha)y^{22}\\&+ (110878540 + 128\alpha)y^{24} + (951037984 + 416\alpha)y^{26}\\&+ (8234878800 - 960\alpha)y^{28} + (50899191200 - 1760\alpha)y^{30} + \cdots,\\W_S =&y^4 + (-1520 - \alpha)y^{16} + (1184890 + 9\alpha)y^{20}\\&+ (205725840 - 153\alpha)y^{24} + \cdots,\end{aligned}$$

respectively, where α is an integer. Hence the weight enumerator of $N_{QR_{104}}(v)$ is completely determined from the number n_3.

By considering all vectors v of weight 4, singly even self-dual $[104, 52, 18]$ codes $N_{QR_{104}}(v)$ with 18 different weight enumerators are constructed. The numbers of codewords of weight 18 are as follows:

$$\begin{aligned}&23208, 23424, 23484, 23616, 23628, 23640, 23652, 23664, 23676,\\&\qquad 23700, 23736, 23748, 23772, 23784, 23796, 23808, 23868, 23988.\end{aligned}$$

Hence we have the following:

Proposition 5. *There are at least* 18 *inequivalent singly even self-dual* $[104, 52, 18]$ *codes. The largest minimum weight among singly even self-dual codes of length* 104 *is* 18 *or* 20.

Remark 6. For $k = 0, 1, \ldots, 4$, an extremal doubly even self-dual $[24k + 8, 12k + 4, 4k + 4]$ code is currently known. However, an extremal singly even self-dual $[24k + 8, 12k + 4, 4k + 4]$ code is currently known for only $k = 1$.

Although an extremal doubly even self-dual code of length 128 is not known, there is a doubly even self-dual $[128, 64, 20]$ code, namely, the extended quadratic residue code QR_{128} of length 128 (see e.g., [18, Fig. 16.2]). Thus a singly even self-dual $[128, 64, d \geq 18]$ code can be constructed by the above construction. We have verified that these singly even self-dual codes $N_{QR_{128}}(v)$ have minimum weight 18 for all vectors v of weight 4. In Section 5, we construct a singly even self-dual $[128, 64, 20]$ code by a different method.

5 Double circulant and four-circulant self-dual codes

Let D_p and D_b be codes with generator matrices of the form

$$(1) \qquad \begin{pmatrix} I_n & R \end{pmatrix}$$

and

(2)
$$\left(\begin{array}{ccccc} & 0 & 1 & \cdots & 1 \\ & 1 & & & \\ I_{n+1} & \vdots & & R' & \\ & 1 & & & \end{array}\right),$$

respectively, where I_n is the identity matrix of order n and R and R' are $n \times n$ circulant matrices. The codes D_p and D_b are called *pure double circulant* and *bordered double circulant*, respectively. These two families are called double circulant codes. Bordered double circulant codes are considered only when the length is divisible by four for self-dual codes. A number of double circulant self-dual codes with large minimum weights are known (see e.g., [21, Table XI]).

By considering double circulant codes, we have found singly even self-dual codes with larger minimum weights than the previously known singly even self-dual codes for lengths $122, 124$ and 130. These codes are listed in Table 3 where the first rows of R and R' in (1) and (2) are written in octal using $0 = (000)$, $1 = (001), \dots,\ 6 = (110)$ and $7 = (111)$, together with $a = (0)$ and $b = (1)$.

Table 3: Double circulant singly even self-dual codes

Codes	Parameters	Types	First rows of R, R'
C_{122}	$[122, 61, 20]$	pure (1)	3724767373745647577736b
C_{124}	$[124, 62, 20]$	bordered (2)	33377772232376476036a
C_{130}	$[130, 65, 20]$	pure (1)	341222607257021041672ba

Let A, B be $n \times n$ circulant matrices with $AA^T + BB^T = I_n$ where A^T denotes the transposed matrix of A. Then the following matrix

(3)
$$\left(\begin{array}{ccc} I_{2n} & A & B \\ & B^T & A^T \end{array}\right)$$

generates a self-dual code of length $4n$ [15]. A code with generator matrix of the form (3) is called a four-circulant code.

By considering four-circulant codes, we have found a singly even self-dual $[128, 64, 20]$ code C_{128} where the first rows r_A and r_B of A and B are given by

$$r_A = (00000000000000000000000101110111),$$
$$r_B = (00010010111110110100010011110111)$$

respectively.

Proposition 7. *There is a singly even self-dual code with minimum weight* 20 *for lengths* $122, 124, 128$ *and* 130*. The largest minimum weights among singly even self-dual codes of lengths* 122 *and* 124 *are* 20 *or* 22*. The largest minimum weight among singly even self-dual codes of lengths* $128, 130$ *are* $20, 22, 24$.

Remark 8. The code C_{122} has the smallest length among all known singly even self-dual codes with minimum weight 20.

Similarly to the previous sections, by 4) in [5, Theorem 5], one can determine the possible weight enumerators of a singly even self-dual code with minimum weight 20 and its shadow for lengths $122, 124, 128$ and 130. To save space, instead of listing the possible weight enumerators, we only give the weight enumerators of $C_{122}, C_{124}, C_{128}, C_{130}$ and their shadows in Appendix. Similarly to previous sections, these weight enumerators are determined by calculating the numbers of codewords of some small weights in the codes and vectors of some small weights in the shadows.

From the weight enumerator of the shadow of C_{130}, the code C_{130} has shadow of minimum weight 21. Hence a singly even self-dual $[132, 66, 20]$ code C_{132} can be constructed by Theorem 1 in [3]. By Lemma 2.2 in [12], C_{132} is equivalent to some bordered double circulant code. More precisely, let R_{130} denote the circulant matrix R in (1) whose first row is given in Table 3 for C_{130}, then the bordered double circulant $[132, 66, 20]$ code has generator matrix of the form (2) with $R' = R_{130} + J$ where J is the 65×65 all-one's matrix.

Appendix

In Appendix, we give the weight enumerators of $C_{122}, C_{124}, C_{128}, C_{130}$ and their shadows.

- C_{122}:

$$
\begin{aligned}
&1 + 40504y^{20} + 833504y^{22} + 14441140y^{24} + 214072119y^{26} + 2586270680y^{28} \\
&+ 25960795288y^{30} + 219075853901y^{32} + 1564125084020y^{34} \\
&+ 9504006041408y^{36} + 49412274116600y^{38} + 220834594415920y^{40} \\
&+ 851791640160968y^{42} + 2845308862653280y^{44} + 8255517456717792y^{46} \\
&+ 20858354044569240y^{48} + 45990544755515312y^{50} + 88651459245343888y^{52} \\
&+ 149610950855761440y^{54} + 221307624817578744y^{56} \\
&+ 287177772256766235y^{58} + 327090617819814992y^{60} + \cdots , \\
&122y^{17} + 386984y^{21} + 114367558y^{25} + 16751580880y^{29} + 1195052746430y^{33} \\
&+ 44180393491848y^{37} + 883339560949122y^{41} + 9863734665439168y^{45} \\
&+ 63000747752486180y^{49} + 234173658832333520y^{53} + 512501876230394332y^{57} \\
&+ 664905510505341664y^{61} + \cdots ,
\end{aligned}
$$

- C_{124}:

$$
\begin{aligned}
&1 + 36051y^{20} + 351482y^{22} + 15460755y^{24} + 114868856y^{26} + 2797860221y^{28} \\
&+ 16748729740y^{30} + 245054582579y^{32} + 1195059547320y^{34} + 11068047329911y^{36} \\
&+ 44180402833266y^{38} + 270247143772023y^{40} + 883339427107680y^{42} \\
&+ 3697099840171248y^{44} + 9863735213124496y^{46} + 29113872688519296y^{48} \\
&+ 63000746325221600y^{50} + 134642002439168310y^{52} + 234173661537182100y^{54} \\
&+ 370918577071670390y^{56} + 512501872315350160y^{58} + 614268389508276191y^{60} \\
&+ 664905514925060552y^{62} + \cdots , \\
&y^{2} + 1830y^{18} + 1209508y^{22} + 343584757y^{26} + 45292811832y^{30} + 2978286811987y^{34} \\
&+ 103096535801812y^{38} + 1955966234164566y^{42} + 20964559886851232y^{46} \\
&+ 129849648756676900y^{50} + 472436065337927560y^{54} + 1020987278111848215y^{58} \\
&+ 1319086740852007504y^{62} + \cdots ,
\end{aligned}
$$

- C_{128}:

$$
\begin{aligned}
&1 + 13024y^{20} + 320512y^{22} + 6518752y^{24} + 107893760y^{26} + 1469363744y^{28} \\
&+ 16720209920y^{30} + 160226846380y^{32} + 1302352537600y^{34} + 9035848504480y^{36} \\
&+ 53803977344000y^{38} + 276262690956384y^{40} + 1228261246620672y^{42} \\
&+ 4745554927466592y^{44} + 15983581208993792y^{46} + 47058043512730944y^{48} \\
&+ 121390540976971776y^{50} + 274913871912485568y^{52} + 547522392265574400y^{54} \\
&+ 960297391979480000y^{56} + 1484888156480481280y^{58} + 2025991464692893504y^{60} \\
&+ 2440617963090440192y^{62} + 2596788462320257062y^{64} \\
&+ 2440617963090440192y^{66} + \cdots, \\
&28576y^{20} + 13091392y^{24} + 2938351968y^{28} + 320450416000y^{32} + 18071749841120y^{36} \\
&+ 552525047121216y^{40} + 9491111198540832y^{44} + 94116083150578176y^{48} \\
&+ 549827752330122816y^{52} + 1920594769299617920y^{56} + 4051982949582894016y^{60} \\
&+ 5193576902188343552y^{64} + 4051982949582894016y^{68} + \cdots,
\end{aligned}
$$

- C_{130}:

$$
\begin{aligned}
&1 + 14820y^{20} + 239200y^{22} + 4866550y^{24} + 84444690y^{26} + 1195427480y^{28} + 14160399812y^{30} \\
&+ 141341763225y^{32} + 1197407548675y^{34} + 8666776384500y^{36} + 53887428543000y^{38} \\
&+ 289196668851610y^{40} + 1345216010815950y^{42} + 5443429581532800y^{44} \\
&+ 19222937313175700y^{46} + 59407062922649000y^{48} + 161053751175916248y^{50} \\
&+ 383808322960607880y^{52} + 805434249367993440y^{54} + 1490576391613268700y^{56} \\
&+ 2435600008912190900y^{58} + 3517171510883065360y^{60} + 4491786997192989000y^{62} \\
&+ 5075541090706863075y^{64} + \cdots, \\
&111800y^{21} + 41722096y^{25} + 8411337480y^{29} + 839432682400y^{33} + 44036959493800y^{37} \\
&+ 1269642358436400y^{41} + 20806002123314200y^{45} + 198831792219798400y^{49} \\
&+ 1129699986919274160y^{53} + 3870268502236978400y^{57} + 8072196934786862800y^{61} \\
&+ 10307252656439079360y^{65} + \cdots,
\end{aligned}
$$

References

[1] A. Baartmans and V. Yorgov, Some new extremal codes of lengths 76 and 78, Proc. 7th Int. Workshop Alg. and Combin. Coding Theory, 18–24 June, 2000, Bulgaria, pp. 51–54.

[2] 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/.

[3] R. Brualdi and V. Pless, Weight enumerators of self-dual codes, *IEEE Trans. Inform. Theory* **37** (1991), 1222–1225.

[4] N. Chigira, M. Harada and M. Kitazume, Extremal self-dual codes of length 64 through neighbors and covering radii, *Des. Codes Cryptogr.* **42** (2007), 93–101.

[5] 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.

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

[7] R. Dontcheva, On the doubly-even self-dual codes of length 96, *IEEE Trans. Inform. Theory* **48** (2002), 557–561.

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

[9] W. Feit, A self-dual even (96, 48, 16) code, *IEEE Trans. Inform. Theory* **20** (1974), 136–138.

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

[11] P. Gaborit, V. Pless, P. Solé and O. Atkin, Type II codes over $\mathbb{F}_4$, *Finite Fields Appl.* **8** (2002), 171–183.

[12] T.A. Gulliver and M. Harada, Weight enumerators of double circulant codes and new extremal self-dual codes, *Des. Codes and Cryptogr.* **11** (1997), 141–150.

[13] S. Han and J.B. Lee, Nonexistence of some extremal self-dual codes, *J. Korea Math. Soc.* **43** (2006), 1357–1369.

[14] M. Harada, An extremal doubly even self-dual code of length 112, (submitted).

[15] M. Harada, W. Holzmann, H. Kharaghani and M. Khorvash, Extremal ternary self-dual codes constructed from negacirculant matrices, *Graphs and Combin.* **23** (2007), 401–417.

[16] M. Harada and T. Nishimura, An extremal singly even self-dual code of length 88, *Advances Math. Comm.* **1** (2007), 261–267.

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

[18] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[19] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. Control* **22** (1973), 188–200.

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

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

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

[23] V. Yorgov, New self-dual codes of length 106, *Congr. Numer.* **162** (2003), 111–117.

[24] R. Yorgova, Constructing self-dual codes using an automorphism group, *IEEE Trans. Inform. Theory* **54** (2008), 3345–3351.