Construction of Some Extremal Self-Dual Codes

T. Aaron Gulliver
Department of Electrical and Computer Engineering
University of Victoria
P.O. Box 3055, STN CSC, Victoria, B.C.
Canada V8W 3P6

Masaaki Harada
Department of Mathematical Sciences
Yamagata University
Yamagata 990-8560, Japan
and
Jon-Lark Kim
Department of Mathematics, Statistics, and Computer Science
322 SEO(M/C 249),
University of Illinois–Chicago
851 S. Morgan, Chicago, IL 60607-7045, USA

November 13, 2000

Abstract

In this correspondence, we consider binary extremal self-dual codes of lengths divisible by eight. A number of new extremal doubly-even self-dual codes of length 88 are constructed. We construct an extremal singly-even self-dual code of length 64 whose weight enumerator was not known to exist. We also relate an extremal doubly-even self-dual code of length divisible by 24 to an optimal singly-even self-dual code of that length.

1 Introduction

In this correspondence, we consider binary self-dual codes. We refer to [11] for basic definitions. A self-dual binary code is called *doubly-even* if all codewords have weight $\equiv 0 \pmod 4$ and *singly-even* if some codeword has weight $\equiv 2 \pmod 4$.

In general, the minimum weight d of a self-dual code of length n is bounded as follows (cf. [15]):

$$\begin{aligned} d &\leq 4\left\lfloor \frac{n}{24} \right\rfloor + 6 \text{ if } n \equiv 22 \pmod{24}, \\ d &\leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4 \text{ otherwise.} \end{aligned}$$

A singly-even self-dual code meeting the above bound is called *extremal* in this correspondence (see [4, 5] for a better bound up to length 100). A doubly-even self-dual code with $d = 4\lfloor \frac{n}{24} \rfloor + 4$ is called *extremal*. A self-dual code is *optimal* if it has the highest minimum weight of any self-dual code of that length. We remark that any self-dual $[24k, 12k, 4k+4]$ code is doubly-even [15]. Thus any singly-even self-dual $[24k, 12k, 4k+2]$ code is optimal.

The purpose of this correspondence is to investigate extremal self-dual codes of lengths divisible by eight. We construct new extremal doubly-even self-dual $[88, 44, 16]$ codes and a new extremal singly-even self-dual $[64, 32, 12]$ code whose weight enumerator was not known to exist. We relate an extremal doubly-even self-dual code of length divisible by 24 to an optimal singly-even self-dual code of that length. Several new optimal singly-even self-dual $[48, 24, 10]$ codes are given as examples.

2 Extremal Doubly-Even Codes of Length 88

In this section, we construct new extremal doubly-even self-dual codes of length 88. The methods used are the double circulant constructions. A pure double circulant code has generator matrix of the following form

$$\left(\begin{array}{cc} I_n & R \end{array} \right),$$

where R is an $n \times n$ circulant matrix and I_n is the identity matrix of order n. A bordered double circulant code has generator matrix of the following form

$$\left(\begin{array}{ccccc} & 0 & 1 & \cdots & 1 \\ & 1 & & & \\ I_n & \vdots & & R & \\ & 1 & & & \end{array} \right),$$

where R is an $(n-1) \times (n-1)$ circulant matrix. Examples of extremal doubly-even self-dual double circulant codes of length 88 are listed in Table 1. The extremal singly-even self-dual

$[86,43,16]$ code C86 in [5] has shadow of minimum weight 15. By Theorem 1 in [3], an extremal doubly-even self-dual code of length 88 is constructed from C86. It follows from [6] that the code is equivalent to $B_{88,1}$ in Table 1.

We now use the following method given in [9] to check the inequivalence of our codes and the known codes. Let C be a self-dual code of length $2n$. Let $M_t = (m_{ij})$ be the $A_t \times 2n$ matrix with rows composed of the codewords of Hamming weight t in C, where A_i denotes the number of codewords of Hamming weight i in C. For an integer k $(1 \le k \le 2n)$, let $n_t(j_1, \dots, j_k)$ be the number of r $(1 \le r \le A_t)$ such that $m_{rj_1} \cdots m_{rj_k} \neq 0$ over $\mathbb{Z}$ for $1 \le j_1 < \cdots < j_k \le 2n$. We consider the set

$$S_t(k) = \{n_t(j_1, \dots, j_k) | \text{ for any } k \text{ distinct columns } j_1, \dots, j_k\}.$$

Let $M_t(k)$ and $m_t(k)$ be the maximum and minimum numbers in $S_t(k)$, respectively.

Only two inequivalent extremal doubly-even codes of length 88 were previously known (cf. [5]). The values $M_{16}(2)$ and $m_{16}(2)$ of the two known codes and our codes are listed in Table 2. Very recently, two other new codes were presented in [12] and [16]. The results for these codes are also given in the table.

It follows from Table 2 that our 30 double circulant codes are new. Therefore we have the following:

Proposition 2.1. *There are at least* 34 *inequivalent extremal doubly-even self-dual codes of length* 88*.*

We now consider self-dual codes of length 86 obtained from the known extremal doubly-even self-dual $[88,44,16]$ codes by subtracting. As described above, the extremal singly-even self-dual $[86,43,16]$ code C86 implies an extremal doubly-even self-dual $[88,44,16]$ code $B_{88,1}$. Hence the converse assertion shows that $B_{88,1}$ has a set of two coordinates such that the corresponding entries in the codewords of weight 16 are 0's (see the value of $m_{16}(2)$ in Table 2). We have verified that this is the only set having two coordinates such that the above property is satisfied. Since the values of $m_{16}(2)$ for the other codes are not zero, only one extremal singly-even self-dual $[86,43,16]$ code is obtained from the known extremal doubly-even self-dual $[88,44,16]$ codes by subtracting.

3 Extremal Singly-Even Codes

3.1 Lengths Divisible by 24

Lemma 3.1 (Harada [8]). *Let* $(\ I_n\ ,\ A\ )$ *be a generator matrix in standard form of a self-dual code* C_{2n} *of length* $2n$*. If the weight of* $x = (x_1, \cdots, x_n)$ *is congruent to* $\equiv n+1$

(mod 2), *then the following matrix*

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

generates a self-dual code C^*_{2n+2} *of length* $2n+2$ *where* $y_i = x_i + 1$.

Rains [15] shows that the existences of an extremal singly-even self-dual $[24k-2, 12k-1, 4k+2]$ code and an extremal doubly-even self-dual $[24k, 12k, 4k+4]$ code are equivalent. As an extension, we have the following result.

Proposition 3.2. *If there is an extremal doubly-even self-dual* $[24k, 12k, 4k+4]$ *code then there is an optimal singly-even self-dual* $[24k, 12k, 4k+2]$ *code.*

Proof. Suppose that there is an extremal doubly-even self-dual $[24k, 12k, 4k+4]$ code C_{24k}. By subtracting, an extremal singly-even self-dual $[24k-2, 12k-1, 4k+2]$ code C_{24k-2} is constructed from C_{24k}. Since C_{24k-2} is a child of C_{24k}, the covering radius of C_{24k-2} is greater than or equal to $4k+3$ (see Theorem 2 in [1]). So, by Fact 5 in [1], there is a coset of weight $4k+1$. Let x be an element in this coset. Without loss of generality, we may assume that x has the form $(x_1, x_2, \ldots, x_{12k-1}, 1, 1, \ldots, 1)$. Then by Lemma 3.1 with x the minimum weight of the extended code C^*_{24k} is $\min\{4k+2, d\}$, where d is the minimum weight of C_{24k-2}. Since C_{24k-2} has minimum weight $4k+2$, it follows that C^*_{24k} has minimum weight $4k+2$ as required. □

Remark. The above argument may be applied to an extremal doubly-even self-dual code with parameters $[24k+8, 12k+4, 4k+4]$ (resp. $[24k+16, 12k+8, 4k+4]$), however, it is not known in general if the resulting singly-even self-dual code with parameters $[24k+8, 12k+4, 4k+2]$ (resp. $[24k+16, 12k+8, 4k+2]$) is extremal or not (e.g., a singly-even self-dual $[56, 28, 10]$ code can be constructed, but it is not known if there is a singly-even self-dual $[56, 28, 12]$ code). However, the argument provides a way to construct singly-even self-dual codes of length $8n$ from doubly-even self-dual codes of that length.

We give some examples to illustrate the above proposition. For length $n = 24$, the extended Golay $[24, 12, 8]$ code C is the unique extremal doubly-even self-dual code. By subtracting any two coordinates of C, we obtain the unique extremal singly-even self-dual $[22, 11, 6]$ code G_{22} in [14]. As in the proof of Proposition 3.2, we extend G_{22} to get the unique optimal singly-even self-dual code Z_{24} in [14].

For length $n = 48$, only the extended quadratic residue code q_{48} is a known extremal doubly-even self-dual code. By subtracting any two coordinates of q_{48}, we obtain an extremal singly-even self-dual code q''_{48} of length 46. Note that all such codes obtained from q_{48} are equivalent since the automorphism group of q_{48} is PSL(2, 47) which is doubly-transitive. The covering radius of q''_{48} is exactly 11. The matrix $G_{46} = (\ I\ ,\ G''_{46}\ )$ was considered as a generator matrix of q''_{48}. In order to save space, the matrix G''_{46} is written in octal using $0 = (000)$, $1 = (001), \dots,\ 6 = (110)$ and $7 = (111)$ along with $a = (0)$:

367334323673343751407720367334305542265055422765333244105542
260433607552546642043360634251452342514750173003447112434471
12547127067537452340513541466224614662246610052261466224a.

By extending the generator matrix G_{46} of q''_{48} with all possible vectors x in Lemma 3.1, we obtained exactly 10 inequivalent optimal singly-even self-dual $[48, 24, 10]$ codes with weight enumerator

$$W_{48} = 1 + 704y^{10} + 8976y^{12} + \cdots .$$

Only one code with W_{48} was given in [3]. The vectors x used for the 10 codes constructed by Lemma 3.1 and their automorphism group orders are listed in Table 3. The inequivalences have been verified by Magma. We remark that recently Ozeki [13] independently constructed 8 inequivalent optimal self-dual $[48, 24, 10]$ codes with weight enumerator W_{48} by reversing the shadow process. The equivalence with the codes obtained here is given in the fourth column of Table 3.

3.2 Length 64

For length 64, two possible weight enumerators are given in [4]:

$$\begin{aligned} W_{64,1} &= 1 + (1312 + 16\beta)y^{12} + (22016 - 64\beta)y^{14} + \cdots \qquad (14 \le \beta \le 284) \\ &\text{and} \\ W_{64,2} &= 1 + (1312 + 16\beta)y^{12} + (23060 - 64\beta)y^{14} + \cdots \qquad (0 \le \beta \le 277). \end{aligned}$$

For $W_{64,1}$ codes exist with $\beta = 18$ and $\beta = 44$, and for $W_{64,2}$ codes exist with $\beta = 32$, $\beta = 40$ and $\beta = 64$ (cf. [5] and the references therein). Recently, a code with $\beta = 14$ in $W_{64,1}$ was given in [2].

By the method given in [7], we have found a new extremal singly-even $[64, 32, 12]$ code C_{64} with generator matrix $(\ I_{32}\ ,\ G_{64}\ )$. C_{64} has weight enumerator $W_{64,2}$ with $\beta = 10$ which was not known to exist. In order to save space, the matrix G_{64} is written in octal using $0 = (000)$, $1 = (001), \dots,\ 6 = (110)$ and $7 = (111)$ along with $b = (1)$:

416311474744367302267047773370360555634153407116234773757656
314176757515443004353242330453107666063056064230474777364700
643421310653244735404172522132244743553214311334753167512415
271365511305301455676124527036535336407760053330374064731343
625416425342007425073452570507462500152313165534131321130317
407765147771600263177634172317774703651 40b.

Acknowledgment. The authors would like to thank Michio Ozeki for sending a copy of [13].

References

[1] E.F. Assmus, Jr. and V. Pless, "On the covering radius of extremal self-dual codes," *IEEE Trans. Inform. Theory,* vol. 29, pp. 359–363, 1983.

[2] K. Betsumiya, T.A. Gulliver, M. Harada and A. Munemasa, "On Type II codes over $\mathbb{F}_4$," (submitted).

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

[4] J.H. Conway and N.J.A. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1319–1333, 1990.

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

[6] T.A. Gulliver and M. Harada, "Weight enumerators of double circulant codes and new extremal self-dual codes," *Des. Codes and Crypt.*, vol. 11, pp. 141–150, 1997.

[7] M. Harada, "Existence of new extremal doubly-even codes and extremal singly-even codes," *Des. Codes and Crypt.*, vol. 8, pp. 273–283, 1996.

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

[9] M. Harada, "New extremal ternary self-dual codes," *Austral. J. Combin.*, vol. 17, pp. 133–145, 1998.

[10] M. Harada and H. Kimura, "On extremal self-dual codes," *Math. J. Okayama Univ.*, vol. 37, pp. 1–14, 1995.

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

[12] A. Otmani, "A new construction of self-dual codes," Proc. 7th Int. Workshop Alg. and Combin. Coding Theory, 18–24 June, 2000, Bulgaria, pp. 255–260.

[13] M. Ozeki, "Reversing the shadow process in the coding theory and its applications," preprint, Nov. 2000.

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

[15] E.M. Rains, "Shadow bounds for self-dual codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 134–139, 1998.

[16] S. Topalova, "Classification of Hadamard matrices of order 44 with automorphisms of order 7," Proc. 7th Int. Workshop Alg. and Combin. Coding Theory, 18–24 June, 2000, Bulgaria, pp. 305–310.

Table 1: New double circulant codes of length 88

Code	First row of R	Type
$B_{88,1}$	0000000100011101111111010001110110100011101	bordered
$B_{88,2}$	1111111111101000110000000000100010001010000	bordered
$B_{88,3}$	1111111111001010000101001000000000011100000	bordered
$B_{88,4}$	1111111101110000100001100001010000001100000	bordered
$B_{88,5}$	1111111011011001001000000000111000100000001	bordered
$B_{88,6}$	1111111011010000010100010100000000100001110	bordered
$B_{88,7}$	1111111010001101100000010001001000000000100101	bordered
$B_{88,8}$	1111111010001100110001100000000000001101100	bordered
$B_{88,9}$	1111111010000010000000110010110000001010101	bordered
$B_{88,10}$	1111111010000000000101001011100001001010001	bordered
$B_{88,11}$	1111101010000100100100001100000000010001000	bordered
$B_{88,12}$	1111101000100000001001000100000000100110010	bordered
$B_{88,13}$	1111100100101110000001100000000100001000000	bordered
$B_{88,14}$	1111100010010000010100100000000001010001100	bordered
$B_{88,15}$	11110101100001000000001001100000000101000100	bordered
$B_{88,16}$	1111111111110101001100011100100000000001100	bordered
$B_{88,17}$	1111111111101010110010101100001100000000010	bordered
$B_{88,18}$	1111111111101000001000100001100101110010100	bordered
$B_{88,19}$	1111111111011100100001010100001000010001011	bordered
$B_{88,20}$	1111111111010100110110100000100000001101100	bordered
$B_{88,21}$	1111111111001110011100000000101100100000101	bordered
$B_{88,22}$	1111111111001010101011000100011110100000000	bordered
$B_{88,23}$	1111111111000101101001110001100010001000100	bordered
$B_{88,24}$	1111111111001000100011000111000100101100010	bordered
$P_{88,1}$	1111110111000000000000100001000000000110001010	pure
$P_{88,2}$	1111110100001100111000000000000000101000000010	pure
$P_{88,3}$	111111010000001001001100000101000001000010000	pure
$P_{88,4}$	11111100001010010010000110011100000000000000	pure
$P_{88,5}$	1111101000011000000010000100101101000000010000	pure
$P_{88,6}$	11111010000100000000010000000011110011000100	pure

Table 2: Extremal doubly-even self-dual codes of length 88

Code	$M_{16}(2)$	$m_{16}(2)$	Code	$M_{16}(2)$	$m_{16}(2)$
[11, Fig. 16.7]	1081	301	[10]	1126	541
[16]	1120	868	[12]	1096	922
$B_{88,1}$	1050	0	$B_{88,2}$	1080	942
$B_{88,3}$	1161	939	$B_{88,4}$	1130	914
$B_{88,5}$	1204	922	$B_{88,6}$	1591	937
$B_{88,7}$	1120	928	$B_{88,8}$	1419	921
$B_{88,9}$	1333	913	$B_{88,10}$	1110	930
$B_{88,11}$	1096	946	$B_{88,12}$	1247	923
$B_{88,13}$	1105	925	$B_{88,14}$	1124	908
$B_{88,15}$	1548	918	$B_{88,16}$	1333	889
$B_{88,17}$	1095	903	$B_{88,18}$	1135	919
$B_{88,19}$	1118	902	$B_{88,20}$	1161	915
$B_{88,21}$	1083	903	$B_{88,22}$	1105	901
$B_{88,23}$	1247	881	$B_{88,24}$	1376	920
$P_{88,1}$	1137	864	$P_{88,2}$	1127	893
$P_{88,3}$	1126	919	$P_{88,4}$	1118	920
$P_{88,5}$	1083	918	$P_{88,6}$	1107	909

Table 3: Optimal singly-even self-dual codes of length 48 with W_{48}

Code	x	Order	Code in [13]
$C_{48,1}$	(11001000000111001011100)	2	C_7
$C_{48,2}$	(00000010110010011110101)	2	C_4
$C_{48,3}$	(01001010001100010101110)	2	C_3
$C_{48,4}$	(01010010100100001010111)	2	C_8
$C_{48,5}$	(11111111000001010000000)	2	C_{11}
$C_{48,6}$	(11100000010000110101110)	4	C_5
$C_{48,7}$	(11010011000101000001101)	4	
$C_{48,8}$	(01010011010101000001101)	4	
$C_{48,9}$	(01001100010100000110111)	4	C_{16}
$C_{48,10}$	(00010001001000111001111)	4	C_{17}