An Extremal Doubly Even Self-Dual Code of Length 112

Masaaki Harada
Department of Mathematical Sciences
Yamagata University
Yamagata 990–8560, Japan
mharada@sci.kj.yamagata-u.ac.jp

Submitted: Dec 29, 2007; Accepted: Aug 24, 2008; Published: Aug 31, 2008
Mathematics Subject Classifications: 94B05

Dedicated to Professor Tatsuro Ito on His 60th Birthday

Abstract

In this note, an extremal doubly even self-dual code of length 112 is constructed for the first time. This length is the smallest length for which no extremal doubly even self-dual code of length $n \not\equiv 0 \pmod{24}$ has been constructed.

1 Introduction

As described in [10], 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 reasons why much work has been done concerning self-dual codes over these fields.

A binary self-dual code C of length n is a code over $\mathbb{F}_2$ satisfying $C = C^\perp$ where the dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{F}_2^n \mid x \cdot y = 0 \text{ for all } y \in C\}$ under the standard inner product $x \cdot y$. 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. It was shown in [8] that the minimum weight d of a doubly even self-dual code of length n is bounded by $d \le 4[n/24] + 4$. A doubly even self-dual code meeting this upper bound is called *extremal*.

The existence of extremal doubly even self-dual codes is known for the following lengths

$$n = 8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 136$$

and their existence was already known some 25 years ago (see [7, Fig. 19.2], [10, p. 273], see also [9] for length 64). We remark that the existence of an extremal doubly even self-dual code of length 72 is a long-standing open question [11] (see [10, Section 12]). 112 is the smallest length for which no extremal doubly even self-dual code of length $n \not\equiv 0 \pmod{24}$ has been constructed.

In this note, an extremal doubly even self-dual $[112, 56, 20]$ code is constructed for the first time. Moreover, this code has a larger minimum weight than the previously known linear $[112, 56]$ codes. For length $n = 110, 112$, singly even self-dual codes with minimum weight 18 are also constructed using the extremal doubly even self-dual code of length 112. These codes have larger minimum weights than the previously known self-dual codes of that length.

2 An Extremal Doubly Even Self-Dual Code of Length 112

Let A, B be the 28×28 circulant matrices with first rows r_A, r_B, respectively, where

$$r_A = (1,0,0,1,0,1,0,0,0,0,0,0,0,0,1,0,1,0,0,1,1,1,1,0,0,1,1,1),$$
$$r_B = (1,0,1,1,1,0,0,1,1,1,1,1,0,0,0,0,1,1,1,1,0,1,1,1,1,0,1,1).$$

Let C_{112} be the code with generator matrix

$$G = \begin{pmatrix} & I_{56} & & \begin{matrix} A & B \\ B^T & A^T \end{matrix} \end{pmatrix},$$

where I_n denotes the identity matrix of order n and A^T is the transposed matrix of A. Since $AB = BA, AA^T + BB^T = I_{28}$ and the sum of the weights of r_A and r_B is 31, C_{112} is a doubly even self-dual code (see [6] for the construction method). If C_{112} contains a codeword c of weight ≤ 16 then c can be expressed as a sum of at most eight rows of G or a sum of at most seven rows of a parity-check matrix

$$H = \begin{pmatrix} \begin{matrix} A^T & B \\ B^T & A \end{matrix} & & I_{56} & \end{pmatrix},$$

since C_{112} is self-dual. We have verified that the weights of the sums of all g rows of G and the sums of h rows of H are greater than or equal to 20 for $g = 1, 2, \dots, 8$ and $h = 1, 2, \dots, 7$. This shows that C_{112} has minimum weight 20 (the minimum weight is also verified by Magma [1]). Therefore C_{112} is an extremal doubly even self-dual code and we have the following:

Theorem 1. *There is an extremal doubly even self-dual code of length* 112.

The code C_{112} has a larger minimum weight than not only the previously known self-dual codes of length 112 but also the previously known linear $[112, 56]$ codes (see [2] and [5]).

The weight enumerator of an extremal doubly even self-dual code is given in [8] for lengths $n \le 200$. We have verified that C_{112} is generated by the codewords of minimum weight. In addition, we have verified by MAGMA that C_{112} has automorphism group $\mathrm{Aut}(C_{112})$ of order 112 which acts transitively on the coordinates. A generator matrix of C_{112} and programs written in MAGMA to verify the above properties can be obtained electronically from `http://sci.kj.yamagata-u.ac.jp/~mharada/Paper/112.magma`.

Now the smallest length for which no extremal doubly even self-dual code of length $n \not\equiv 0 \pmod{24}$ is known is 128 and the largest length for which an extremal doubly even self-dual code is known is 136.

3 Related Singly Even Self-Dual Codes

The minimum weight d of a singly even self-dual code of length n is bounded by $d \le 4[n/24] + 4$, unless $n \equiv 22 \pmod{24}$ when $d \le 4[n/24] + 6$ or $n \equiv 0 \pmod{24}$ when $d \le 4[n/24] + 2$ (see [10]). A singly even self-dual code meeting this upper bound is called *extremal*.

3.1 Length 110

Let $S_{C_{112}}(i, j)$ be the code obtained by subtracting two coordinates i, j (i.e., taking all codewords with $(0, 0)$, $(1, 1)$ in the coordinates and deleting the coordinates) from C_{112}. The codes $S_{C_{112}}(i, j)$ are self-dual codes of length 110 and minimum weight 18 or 20.

Let $M = (m_{ij})$ be the 355740×112 matrix with rows composed of the codewords of weight 20 in C_{112}. Let $n_{11}^{(j)}$ and $n_{00}^{(j)}$ be the numbers of integers r $(1 \le r \le 355740)$ with $m_{r1} = m_{rj} = 1$ and $m_{r1} = m_{rj} = 0$, respectively, for j $(2 \le j \le 112)$. It is enough to consider only the case $i = 1$ since $\mathrm{Aut}(C_{112})$ acts transitively on the coordinates. We have verified that $n_{11}^{(j)}$ are positive for all j $(2 \le j \le 112)$. Hence the codes $S_{C_{112}}(i, j)$ obtained by subtracting all pairs of two coordinates have minimum weight 18, that is, these self-dual codes are non-extremal. However, these self-dual $[110, 55, 18]$ codes have larger minimum weights than the previously known self-dual codes of length 110 (see [4, Table 2]). By comparing $n_{11}^{(j)}$ and $n_{00}^{(j)}$ for all j, it turns out that over 50 self-dual $[110, 55, 18]$ codes obtained by subtracting have different weight enumerators.

3.2 Length 112

Recall that 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 $v \in \mathbb{F}_2^{112}$ be a vector of weight 4. Then

$$N_{C_{112}}(v) = (C_{112} \cap \langle v \rangle^{\perp}) \cup \{u + v \mid u \in (C_{112} \setminus (C_{112} \cap \langle v \rangle^{\perp}))\}$$

is a singly even self-dual neighbor of C_{112} with minimum weight 18 or 20 (see [3] for the construction method).

Let $M = (m_{ij})$ be the 355740×112 matrix as above. We denote the support of v by $\mathrm{supp}(v) = \{i_1, i_2, i_3, i_4\}$. Let $n_j^{(v)}$ be the number of integers r $(1 \le r \le 355740)$ with

$$\mathrm{wt}(m_{ri_1}, m_{ri_2}, m_{ri_3}, m_{ri_4}) = j \ (j = 0, 1, 2, 3, 4),$$

where $\mathrm{wt}(x)$ denotes the weight of a vector x. From the construction, the numbers of codewords of weights 18 and 20 in $N_{C_{112}}(v)$ are given by $n_3^{(v)}$ and $n_0^{(v)} + n_2^{(v)} + n_4^{(v)}$, respectively. We have verified that $n_3^{(v)}$ are positive for all v with $\mathrm{supp}(v) = \{1, i_2, i_3, i_4\}$. Hence the codes $N_{C_{112}}(v)$ have minimum weight 18, that is, these codes are non-extremal. However, these singly even self-dual $[112, 56, 18]$ codes have larger minimum weights than the previously known singly even self-dual codes of length 112 (see [4, Table 2]). By comparing $n_3^{(v)}$ and $n_0^{(v)} + n_2^{(v)} + n_4^{(v)}$ for all v with $\mathrm{supp}(v) = \{1, 2, i_3, i_4\}$, it turns out that over 100 singly even self-dual $[112, 56, 18]$ neighbors $N_{C_{112}}(v)$ have different weight enumerators.

For lengths $n = 110, 112$, singly even self-dual codes with minimum weight 18 have been constructed. Hence the largest minimum weight among singly even self-dual codes of length n is 18 or 20.

Acknowledgment. The author would like to thank T. Aaron Gulliver and Radinka Yorgova for useful conversations.

References

[1] W. Bosma and J. Cannon, Handbook of Magma Functions, Available online at "`http://magma.maths.usyd.edu.au/magma/`".

[2] A.E. Brouwer, "Bounds on the size of linear codes," in Handbook of Coding Theory, V.S. Pless and W.C. Huffman (Editors), Elsevier, Amsterdam 1998, pp. 295–461.

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

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

[5] M. Grassl, Code tables: Bounds on the parameters of various types of codes, Available online at "`http://www.codetables.de/`".

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

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

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

[9] G. Pasquier, A binary extremal doubly even self-dual code (64, 32, 12) obtained from an extended Reed–Solomon code over F_{16}, *IEEE Trans. Inform. Theory* **27** (1981), 807–808.

[10] 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.

[11] N.J.A. Sloane, Is there a $(72, 36)$ $d = 16$ self-dual code? *IEEE Trans. Inform. Theory* **19** (1973), 251.