Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 125-128*

Construction of a self-dual $[94, 47, 16]$ code

Masaaki Harada
Department of Mathematical Sciences, Yamagata University,
Yamagata 990–8560, JAPAN

Radinka Yorgova[1] radinka@ii.uib.no
Department of Informatics, University of Bergen
Thormøhlensgate 55, N-5008, Bergen, NORWAY

Abstract. The existences of an extremal doubly even self-dual $[96, 48, 20]$ code and a self-dual $[94, 47, 18]$ code are equivalent. The largest minimum weight among self-dual codes of length 94 was previously known as $14, 16$ or 18. In this note, a self-dual $[94, 47, 16]$ code is constructed for the first time.

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. It was shown in [9] that the minimum weight d of a doubly even self-dual code of length n is bounded by $d \le 4[n/24] + 4$. In [10] 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 $d \le 4[n/24] + 6$ or $n \equiv 0 \pmod{24}$ when $d \le 4[n/24] + 2$.

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 [10] 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 [4, Table VI], [6, Table 2]).

In this note, a self-dual $[94, 47, 16]$ code is constructed for the first time. Hence the largest minimum weight among self-dual codes of length 94 is 16 or 18.

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

2.1 Construction

An automorphism of 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. Extremal doubly even self-dual codes with automorphisms of a fixed odd prime order have been widely investigated (see e.g., [8], [11]).

Suppose that σ is an automorphism of order 23 of a self-dual $[94, 47, 16]$ code. By [11, Theorem 1], one can show that σ consists of four 23-cycles together with two fixed points. Using the technique developed by Huffman [8] and Yorgov [11], 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:

M	r	M	r
e_1	(10000101001100110101111)	e_2	(11010001001111110100100)
e_3	(10001110110000111010101)	e_4	(10001000010001010011100)
f_1	(11111010110011001010000)	f_2	(10010010111111001000101)
f_3	(11010101110000110111000)	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.

Remark 2 *The largest minimum weight among known linear* $[94, 47]$ *codes is currently* 16 *(see [7]).*

2.2 Weight enumerators

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 $C_0^\perp \setminus C$ [2]. 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 Theorem 5, 4) in [2], a self-dual $[94, 47, 16]$ code C and its shadow S have the following possible weight enumerators:

$$\begin{aligned}W_C =&1 + 2\alpha y^{16} + (134044 - 2\alpha + 128\beta)y^{18}\\&+ (2010660 - 30\alpha - 896\beta + 8192\gamma)y^{20}\\&+ (22385348 + 30\alpha + 1280\beta - 106496\gamma - 5242888\delta)y^{22}\\&+ (207307788 + 210\alpha + 5376\beta + 581632\gamma + 9961472\delta)y^{24}\\&+ (1545393276 - 210\alpha - 18048\beta - 1597440\gamma - 880803840\delta)y^{26} + \cdots ,\\W_S =&\delta y^3 + (\gamma - 22\delta)y^7 + (-\beta - 20\gamma + 231\delta)y^{11}\\&+ (\alpha + 18\beta + 190\gamma - 1540\delta)y^{15}\\&+ (1072352 - 16\alpha - 153\beta - 1140\gamma + 7315\delta)y^{19}\\&+ (140151744 + 120\alpha + 816\beta + 4845\gamma - 26334\delta)y^{23} + \cdots ,\end{aligned}$$

respectively, where $\alpha, \beta, \gamma, \delta$ are integers. By Theorem 5, 3) in [2], 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.

We have verified that the number of codewords of weight 16 in C_{94} is 6072 and that the minimum weight of the shadow is 15. Hence the weight enumerator of the code C_{94} corresponds to $(\alpha, \beta, \gamma, \delta) = (3036, 0, 0, 0)$. We have verified by MAGMA that C_{94} has automorphism group of order 23.

2.3 A related self-dual code of length 96

Let C be a singly even self-dual code of length $n \equiv 6 \pmod 8$. Let C^* be the code of length $n + 2$ obtained by extending $C_0^\perp$ as follows:

$$(0, 0, C_0) \cup (1, 1, C_2) \cup (1, 0, C_1) \cup (0, 1, C_3)$$

where (x, y, C_i) denotes the set $\{(x, y, z) \in \mathbb{F}_2^{n+2} | z \in C_i\}$. Then C^* is a doubly even self-dual code [1]. In our case, C_{94}^* is a doubly even self-dual $[96, 48, 16]$ code since C_{94} has shadow of minimum weight 15. The code C_{94}^* has the following weight enumerator:

$$\begin{aligned}&1 + 9108y^{16} + 3071328y^{20} + 370937840y^{24} + 18637739040y^{28}\\&+ 422086556775y^{32} + 4552826872672y^{36} + 24292762502544y^{40}\\&+ 65726907444000y^{44} + 91447786444040y^{48} + \cdots + y^{96}.\end{aligned}$$

There are 30 known inequivalent doubly even self-dual $[96, 48, 16]$ codes [3], [4] and [5]. Since C_{94}^* and the 30 known codes have different weight enumerators, C_{94}^* is inequivalent to any of the known codes. We have verified by MAGMA that C_{94}^* has automorphism group of order 23.

References

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

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

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

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

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

[6] P. Gaborit, A. Otmani, Experimental constructions of self-dual codes, *Finite Fields Appl.* 9, 2003, 372-394.

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

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

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

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

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