On the covering radii of extremal doubly even self-dual codes

著者	Harada Masaaki, Munemasa Akihiro
journal or publication title	Advances in Mathematics of Communications
volume	1
number	2
page range	251-256
year	2007
URL	http://hdl.handle.net/10097/51630

doi: 10.3934/amc.2007.1.251

Advances in Mathematics of Communications
Volume 1, No. 2, 2007, 251–256 Web site: http://www.aimSciences.org

ON THE COVERING RADII OF EXTREMAL DOUBLY EVEN SELF-DUAL CODES

Masaaki Harada

Department of Mathematical Sciences
Yamagata University, Yamagata 990–8560, Japan

Akihiro Munemasa

Graduate School of Information Sciences
Tohoku University, Sendai 980–8579, Japan

(Communicated by Iwan Duursma)

Abstract. In this note, we study the covering radii of extremal doubly even self-dual codes. We give slightly improved lower bounds on the covering radii of extremal doubly even self-dual codes of lengths $64, 80$ and 96. The covering radii of some known extremal doubly even self-dual $[64, 32, 12]$ codes are determined.

1. Introduction

The covering radius $R(C)$ of a binary code C of length n is the smallest integer R such that spheres of radius R around codewords of C cover the space $\mathbb{F}_2^n$ where $\mathbb{F}_2$ is the finite field of order 2. The covering radius is a basic and important geometric parameter of a code. A vector a of a coset $U = x + C$ is called a coset leader of U if the weight of a is minimal in U, and the weight of a coset U is defined as the weight of a coset leader. The covering radius $R(C)$ is the same as the maximum of weights of all the nontrivial cosets of C.

A code C is called *self-dual* if $C = C^\perp$ where $C^\perp$ is the dual code of C. A binary self-dual code C is called *doubly even* if all codewords have weight $\equiv 0 \pmod 4$ and *singly even* if some codeword has weight $\equiv 2 \pmod 4$. The minimum weight d of a self-dual code C of length n is bounded by $d \leq 4[n/24] + 4$ unless $n \equiv 22 \pmod{24}$ when $d \leq 4[n/24] + 6$ [14, 17]. We call a self-dual code meeting this upper bound *extremal*.

Assmus and Pless [1] studied the covering radii of extremal doubly even self-dual codes. In particular, they determined the covering radii of extremal doubly even self-dual codes of lengths up to 32 and length 48, and gave bounds for lengths $40, 56, 64, \dots, 96$.

In this note, we investigate the covering radii of extremal doubly even self-dual codes. In Section 2, we give a lower bound on covering radii of linear codes which is a sharpening of the sphere-covering bound. Although our bound does not lead to an improvement over the one obtained by [6, (2)] for lengths up to 96, we remark that the bound obtained by [6, (2)] improves the published lower bounds on the covering radii of extremal doubly even self-dual codes of lengths $64, 80$ and 96. In Section 3, we relate the covering radii to singly even neighbors. Namely we establish a

2000 *Mathematics Subject Classification:* Primary: 94B05; Secondary: 94B75.
Key words and phrases: Extremal doubly even self-dual code, covering radius, neighbor.

Length n	$R(C_n)$	Length n	$R(C_n)$
8	2	56	8–10
16	4	64	9–12
24	4	72	10–12
32	6	80	11–14
40	6–8	88	12–16
48	8	96	13–16

TABLE 1. Bounds on covering radii of extremal doubly even self-dual codes

relationship between extremal singly even self-dual codes with shadow of minimum weight $4\mu+4$ and extremal doubly even self-dual codes with covering radius $4\mu+4$, for length $24\mu+16$. In Section 4, the covering radii of some known extremal doubly even self-dual codes are determined for length 64. From the results for lengths up to 56 (see Section 2), the Delsarte bound seems to give a rather good upper bound on the covering radii of extremal doubly even self-dual codes. However, our calculation indicates that the covering radii of many extremal doubly even self-dual codes of length 64 do not meet the Delsarte bound. We do not know any other published result of determination of the covering radii of extremal doubly even self-dual codes of length 64, and 64 seems to be the smallest length for which the Delsarte bound is rarely met.

2. BOUNDS ON COVERING RADII

Assmus and Pless [1] gave bounds on the covering radii of extremal doubly even self-dual codes of lengths up to 96. In this section, we investigate covering radii of (extremal) doubly even self-dual codes. A simple counting gives the following sphere-covering bounds for even codes.

Proposition 1 (cf. [6, (2)])**.** *Let C be an even $[n,k]$ code. Then*

$$\sum_{2i\le R(C)} \binom{n}{2i} \ge 2^{n-k-1} \text{ and } \sum_{2i+1\le R(C)} \binom{n}{2i+1} \ge 2^{n-k-1}.$$

Let C_n be an extremal doubly even self-dual code of length n. According to the published results, it is known that $8 \le R(C_{64})$, $10 \le R(C_{80})$ and $12 \le R(C_{96})$ [1, Table III] (see also [4, Table 5], [12, Table 11.5], [16, Table II]). Using Proposition 1, we give slightly improved bounds.

Proposition 2. *Let C_n be an extremal doubly even self-dual code of length n. Then $9 \le R(C_{64})$, $11 \le R(C_{80})$ and $13 \le R(C_{96})$.*

Proof. Since $\binom{64}{1}+\binom{64}{3}+\binom{64}{5}+\binom{64}{7} < 2^{31}$, $R(C_{64}) \ge 9$ by Proposition 1. The others are similar. □

We list in Table 1 the bound on the covering radius of an extremal doubly even self-dual code of length $n \le 96$. We remark that the covering radius for length 16 was incorrectly reported as 2 in [1, Table III], reproduced in [4, Table 5], [16, Table II], and then corrected in [12, Table 11.5].

We now give a sharpening of Proposition 1.

Proposition 3. *Let C be a code of length n with weight enumerator $\sum_{i=0}^{n} A_i y^i$. If C has covering radius r, then*

$$\binom{n}{w} \le \sum_{i=0}^{n} A_i \sum_{\substack{0\le j\le r \\ j\equiv i+w \pmod 2}} \binom{i}{\frac{i+w-j}{2}}\binom{n-i}{w-\frac{i+w-j}{2}},$$

for all integers w with $0 \le w \le n$.

Proof. Let $\mathrm{wt}(x)$ denote the weight of a vector $x \in \mathbb{F}_2^n$. Then

$$\begin{aligned}
\binom{n}{w} &= |\bigcup_{x\in C}\{z \in \mathbb{F}_2^n \mid \mathrm{wt}(z)=w,\ \mathrm{wt}(x-z)\le r\}| \\
&\le \sum_{x\in C} |\{z \in \mathbb{F}_2^n \mid \mathrm{wt}(z)=w,\ \mathrm{wt}(x-z)\le r\}| \\
&= \sum_{i=0}^{n} \sum_{\substack{x\in C\\ \mathrm{wt}(x)=i}} \sum_{j=0}^{r} |\{z \in \mathbb{F}_2^n \mid \mathrm{wt}(z)=w,\ \mathrm{wt}(x-z)= j\}| \\
&= \sum_{i=0}^{n} \sum_{\substack{x\in C\\ \mathrm{wt}(x)=i}} \sum_{\substack{0\le j\le r \\ j\equiv i+w \pmod 2}} \binom{i}{\frac{i+w-j}{2}}\binom{n-i}{w-\frac{i+w-j}{2}} \\
&= \sum_{i=0}^{n} A_i \sum_{\substack{0\le j\le r \\ j\equiv i+w \pmod 2}} \binom{i}{\frac{i+w-j}{2}}\binom{n-i}{w-\frac{i+w-j}{2}}.
\end{aligned}$$

□

We remark that, Proposition 1 follows from Proposition 3 by taking the sum of the inequalities for all even (or odd) w. Proposition 3 generalizes the argument given in the proof of [1, Theorem 3]. It gives $R(C_{32}) \ge 6$ for an extremal doubly even self-dual code C_{32} of length 32 by taking $w = 6$, while Proposition 1 only gives $R(C_{32}) \ge 5$. We do not know, however, that Proposition 3 gives a stronger bound than Proposition 1 for extremal doubly even self-dual codes for length other than 32.

If we do not restrict our attention to extremal doubly even self-dual codes, there are cases where the bound in Proposition 3 is stronger than the one in Proposition 1. Indeed, let Z_{24} be the unique singly even self-dual $[24, 12, 6]$ code. The code Z_{24} has weight enumerator

$$1 + 64y^6 + 375y^8 + 960y^{10} + 1296y^{12} + \cdots + y^{24}.$$

Applying Proposition 3 with $w = 5$ gives the bound $R(Z_{24}) \ge 5$, while Proposition 1 only gives $R(Z_{24}) \ge 4$. In fact, it is known that Z_{24} has covering radius 5 (cf. [3]).

Also, if D_{32} is a doubly even self-dual $[32, 16, 4]$ code having $1, 2$ or at least 65 codewords of weight 4, then we have $R(D_{32}) \ge 6$ by taking $w = 6, 6$ or 12, respectively, in Proposition 3, while Proposition 1 only gives $R(D_{32}) \ge 5$. However, since all doubly even self-dual $[32, 16, 4]$ codes have been classified [18], one can directly determine the covering radius for all such codes. In fact, we have verified that every doubly even self-dual $[32, 16, 4]$ code has covering radius $6, 7$ or 8.

For lengths up to 32 and length 48, the covering radius of an extremal doubly even self-dual code is uniquely determined (see Table 1). For length 40, a large number of inequivalent extremal doubly even self-dual codes are known, however, only two extremal doubly even self-dual codes with covering radius 7 which does not meet the Delsarte bound are known (cf. [11]). By the Delsarte bound, the covering radius of an extremal doubly even self-dual code of length 56 is at most 10. By finding a coset of weight 10, the covering radius of $D11$ in [7] was determined as 10 in [20]. Similarly, we have verified that more than one thousand extremal doubly even self-dual $[56, 28, 12]$ codes found in [9] and [10] have covering radius 10. We do not know whether there exists an extremal doubly even self-dual $[56, 28, 12]$ code with covering radius 8 or 9.

From known covering radii for lengths up to 56, the Delsarte bound seems to give a rather good upper bound on the covering radii of extremal doubly even self-dual codes. However, as we shall see in Section 4, the covering radii of many extremal doubly even self-dual codes of length 64 do not meet the Delsarte bound.

3. Length $24\mu + 16$

In this section, we establish a relationship between extremal singly even self-dual codes with shadow of minimum weight $4\mu + 4$ and extremal doubly even self-dual codes with covering radius $4\mu + 4$, for length $24\mu + 16$.

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 by Conway and Sloane [7], to be $C_0^\perp \setminus C$. 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 $S = C_1 \cup C_3$ [7]. Two self-dual codes C and C' of length n are said to be *neighbors* if the dimension $\dim C \cap C'$ is $n/2 - 1$. If C is a singly even self-dual code of length divisible by eight then C has two doubly even self-dual neighbors, namely, $C_0 \cup C_1$ and $C_0 \cup C_3$.

Lemma 3.1. *Let C_0 be a doubly even $[24\mu + 16, 12\mu + 7, 4\mu + 4]$ code. Let D_1, D_2 (resp. C) be the doubly even self-dual codes (resp. the singly even self-dual code) containing C_0. The following statements are equivalent:*

(i) *the minimum weight of $C_0^\perp$ is $4\mu + 4$,*
(ii) *for at least one of $i = 1, 2$, the minimum weight of D_i and that of $C_0^\perp \setminus D_i$ are both $4\mu + 4$,*
(iii) *for each of $i = 1, 2$, the minimum weight of D_i and that of $C_0^\perp \setminus D_i$ are both $4\mu + 4$,*
(iv) *the minimum weight of C and that of its shadow are both $4\mu + 4$.*

Proof. Let S be the shadow of C. Then we have

$$C_0^\perp = C \cup S = D_1 \cup (C_0^\perp \setminus D_1) = D_2 \cup (C_0^\perp \setminus D_2). \tag{1}$$

A self-dual code of length $24\mu + 16$ has minimum weight at most $4\mu + 4$. The minimum weight of the shadow of an extremal singly even self-dual code of length $24\mu + 16$ is at most $4\mu + 4$ [2]. By the Delsarte bound, the covering radius of an extremal doubly even self-dual code is at most $4\mu + 4$. By these bounds, each part of the three decompositions (1) of $C_0^\perp$ has minimum weight at most $4\mu + 4$. We then see that each of the three assertions (ii)–(iv) are equivalent to (i). □

The following proposition characterizes the Delsarte bound for extremal doubly even self-dual $[24\mu + 16, 12\mu + 8, 4\mu + 4]$ codes.

Proposition 4. *If D is an extremal doubly even self-dual $[24\mu + 16, 12\mu + 8, 4\mu + 4]$ code with covering radius $4\mu + 4$, then D has an extremal singly even self-dual $[24\mu + 16, 12\mu + 8, 4\mu + 4]$ neighbor whose shadow has minimum weight $4\mu + 4$.*

Conversely, if C is an extremal singly even self-dual $[24\mu+16, 12\mu+8, 4\mu+4]$ code whose shadow has minimum weight $4\mu+4$, then the two doubly even self-dual neighbors of C are both extremal doubly even self-dual $[24\mu+16, 12\mu+8, 4\mu+4]$ codes with covering radius $4\mu+4$.

Proof. Suppose that D is an extremal doubly even self-dual $[24\mu+16, 12\mu+8, 4\mu+4]$ code with covering radius $4\mu+4$. Then there is a coset $w+D$ of weight $4\mu+4$. Define C_0 by $C_0 = (D \cup (w+D))^\perp$. Then Lemma 3.1 implies that the singly even self-dual code C containing C_0 is an extremal neighbor of D whose shadow has minimum weight $4\mu+4$. The converse is immediate from Lemma 3.1. □

4. LENGTH 64

In this section, we determine the covering radii of some known extremal doubly even self-dual codes of length 64.

It is known that there are precisely four inequivalent extremal doubly even self-dual $[64, 32, 12]$ codes constructed from symmetric 2-$(31, 10, 3)$ designs [13]. The design No. 2 in [19] gives rise to a code D with the largest automorphism group among the four codes. There are exactly 45 (resp. 21) inequivalent pure (resp. bordered) double circulant extremal doubly even self-dual codes of length 64 [8]. These codes are denoted by $P_1, \dots, P_{45}$ (resp. $B_1, \dots, B_{21}$) in [8]. We determine the covering radii of these codes as follows. Due to computer time limitations, we have only been able to accomplish our search in extremal doubly even self-dual codes with relatively large automorphism groups.

By the Delsarte bound, the covering radius of an extremal doubly even self-dual code of length 64 is at most 12. By modifying the method in [15], we have verified that there is no coset of weight 12 for the codes D, $P_1, \dots, P_{45}$, $B_1, \dots, B_{21}$. Similarly, we have found a coset of weight 11 for the codes D, P_i and B_j where

$$i \in \Gamma_P = \{3, 4, 8, 10, 11, 13, 15, 16, 20, 23, 24, 25, 30, 33, 35, 41, 43\},$$
$$j \in \Gamma_B = \{1, 2, 3, 4, 5, 8, 9, 10, 11, 14, 15, 21\},$$

and there is no coset of weight 11 for the remaining codes. Moreover, we have found a coset of weight 10 for the remaining codes. Hence we have the following:

Theorem 4.1. *The covering radii of the codes D, P_i B_j are 11 for $i \in \Gamma_P$ and $j \in \Gamma_B$. The covering radii of the codes P_i, B_j are 10 for $i \notin \Gamma_P$ and $j \notin \Gamma_B$*

Theorem 4.1 indicates that there are many extremal doubly even self-dual codes with covering radius not meeting the Delsarte bound (compare with lengths 40 and 56). Recently an extremal singly even self-dual $[64, 32, 12]$ code with shadow of minimum weight 12 was found in [5], after a manuscript of this note was first circulated. By Proposition 4, this leads to an extremal doubly even self-dual $[64, 32, 12]$ code with covering radius 12. We do not know whether there exists an extremal doubly even self-dual $[64, 32, 12]$ code with covering radius 9.

By Corollary 2 to Theorem 1 in [1], the cosets of weights 11 and 12, if there are any, have unique weight enumerators. The unique weight enumerator for weight 11 is:

$$\begin{aligned} &312y^{11} + 6392y^{13} + 74512y^{15} + 640272y^{17} + 4060312y^{19} + 19150296y^{21} \\ &+ 68319936y^{23} + 186730176y^{25} + 394257136y^{27} + 646744176y^{29} \\ &+ 827500128y^{31} + \cdots \end{aligned}$$

(see [5] for weight 12).

Acknowledgements

The authors would like to thank Kenichiro Tanabe for suggesting a room for improvement on lower bounds on the covering radius of extremal doubly even self-dual codes, which lead to the discovery of the results in the present note.

References

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

[2] C. Bachoc, P. Gaborit, *Designs and self-dual codes with long shadows,* J. Combin. Theory, Ser. A, **105** (2004), 15–34.

[3] D. J. Bergstrand, *New uniqueness proofs for the* (5, 8, 24), (5, 6, 12) *and related Steiner systems*, J. Combin. Theory, Ser. A, **33** (1982), 247–272.

[4] R. Brualdi, S. Litsyn and V. Pless, *Covering radius*, in "Handbook of Coding Theory" (eds. V. S. Pless and W. C. Huffman), Elsevier, Amsterdam, (1998), 755–826.

[5] 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.

[6] G. D. Cohen, M. G. Karpovsky, H. F. Mattson, Jr. and J. R. Schatz, *Covering radius – Survey and recent results*, IEEE Trans. Inform. Theory, **31** (1985), 328–343.

[7] 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.

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

[9] M. Harada, *Self-orthogonal* 3-$(56, 12, 65)$ *designs and extremal doubly-even self-dual codes of length* 56*,* Des. Codes Cryptogr., **38** (2006), 5–16.

[10] M. Harada, T. A. Gulliver and H. Kaneta, *Classification of extremal double-circulant self-dual codes of length up to* 62*,* Discrete Math., **188** (1998), 127–136.

[11] M. Harada, A. Munemasa and K. Tanabe, *Extremal self-dual* $[40, 20, 8]$ *codes with covering radius* 7*,* Finite Fields Appl., **10** (2004), 183–197.

[12] W. C. Huffman, V. Pless, "Fundamentals of Error-Correcting Codes," Cambridge University Press, Cambridge, 2003.

[13] S. N. Kapralov, V. D. Tonchev, *Extremal doubly-even codes of length* 64 *derived from symmetric designs*, Discrete Math., **83** (1990), 285–289.

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

[15] A. Munemasa, *On the enumeration of self-dual codes*, "Proceedings of the Fourth Conference on Algebraic Geometry, Number Theory, Coding Theory and Cryptography," University of Tokyo, (2000), 69–77.

[16] M. Ozeki, *Jacobi polynomials for singly even self-dual codes and the covering radius problems,* IEEE Trans. Inform. Theory, **48** (2002), 547–557.

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

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

[19] V. D. Tonchev, *Symmetric* 2-$(31, 10, 3)$ *designs with automorphisms of order seven,* Annals of Discrete Math., **34** (1987), 461–464.

[20] H. -P. Tsai, *The covering radius of extremal self-dual code D*11 *and its application,* IEEE Trans. Inform. Theory, **43** (1997), 316–319.

Received December 2006; revised March 2007.

E-mail address: mharada@sci.kj.yamagata-u.ac.jp
E-mail address: munemasa@math.is.tohoku.ac.jp