A Note on Formally Self-Dual Even Codes of Length Divisible by 8

Jon-Lark Kim
Department of Mathematics
328 Natural Sciences Building
University of Louisville
Louisville, KY 40292, USA
e-mail: jl.kim@louisville.edu

Vera Pless
Department of Mathematics, Statistics, and Computer Science
322 SEO(M/C 249)
University of Illinois–Chicago
851 S. Morgan, Chicago, IL 60607-7045, USA
e-mail: pless@math.uic.edu

Abstract

A binary code with the same weight distribution as its dual code is called *formally self-dual (f.s.d.)*. We only consider f.s.d. even codes (codes with only even weight codewords). We show that any formally self-dual even binary code $\mathcal{C}$ of length n not divisible by 8 is balanced. We show that the weight distribution of a balanced near-extremal f.s.d. even code of length a multiple of 8 is unique. We also determine the possible weight enumerators of a near-extremal f.s.d. even $[n, n/2, 2\lfloor n/8 \rfloor]$ code with $8 \mid n$ as well as the dimension of its radical.

Keywords Formally self-dual code, self-dual code.

1 Introduction

Self-dual codes are an interesting class of codes [13]. In particular, binary, ternary, and quaternary self-dual codes have been extensively studied due to the Gleason-

Pierce-Ward theorem [14],[15, pp. 857].

A binary formally self-dual (f.s.d.) code is a binary code with the same weight distribution as its dual code. We only consider a f.s.d. *even* code, i.e., all weights of codewords are even. There are two types of binary self-dual codes: *Type II*, the doubly-even codes where all weights are divisible by 4, and *Type I*, the singly-even codes where some weights are also equivalent to 2 (mod 4).

One reason of interest in extremal f.s.d. even codes is that sometimes a f.s.d. even code can have a larger minimum weight than a self-dual code of the same length. One can also obtain designs from vectors of a fixed weight in an extremal f.s.d. even code by the Assmus-Mattson theorem. Further in extremal f.s.d. even codes of length $n \equiv 2 \pmod 8$ (resp. $n \equiv 6 \pmod 8$), the words of a fixed weight in $\mathcal{C} \cup \mathcal{C}^{\perp}$ hold a 3-design (resp. 1-design) [10]. However as the code length n goes up, say $n \geq 32$, there do not exist extremal f.s.d. even codes and so we consider near extremal f.s.d. even codes. There are a few papers [1],[6],[7] dealing with near extremal f.s.d. even codes.

In this paper, we show that any f.s.d. even binary code $\mathcal{C}$ of length n not divisible by 8 is balanced. We show that the weight distribution of a balanced near-extremal f.s.d. even code of length a multiple of 8 is unique. This gives an elementary explanation of the fact that the weight distribution of the three Type I self-dual $[32, 16, 8]$ codes is unique [4]. We also determine the possible weight enumerators of a near-extremal f.s.d. even $[n, n/2, 2\lfloor n/8 \rfloor]$ code with $8 \mid n$ as well as the dimension of its radical.

2 Near-extremal formally self-dual even codes

Throughout this section, let $\mathcal{C}$ be a formally self-dual even binary code of length n. Let $W_1 = (x^2 + y^2)$ and $W_2 = x^2y^2(x^2 - y^2)^2$ be homogeneous polynomials in x and y of degrees 2 and 8 respectively, called *Type I Gleason polynomials*. It is a well known fact that the weight enumerator $W_{\mathcal{C}}(x, y)$ of a f.s.d. even binary code $\mathcal{C}$ is a combination of W_1 and W_2. By this fact, the minimum weight d of any f.s.d. even $[n, n/2, d]$ code is bounded by $d \leq 2\lfloor n/8 \rfloor + 2$. A f.s.d. even code meeting this bound is called *extremal*. A f.s.d. even code with $d^* = 2\lfloor n/8 \rfloor$ is called *near-extremal* [7]. This is the actual bound for Type I codes with $n \geq 16$ and for all f.s.d. even codes with $n \geq 32$ [6].

A vector is *doubly-even* if its weight is divisible by 4 and *singly-even* if its weight is even but not divisible by 4. We call an even binary code *balanced* [9] if it contains the same number of doubly-even vectors and singly-even vectors. Any Type I self-dual code is balanced. We denote the set of doubly-even vectors of $\mathcal{C}$ by $\mathbf{DE}$ and the set of singly-even vectors of $\mathcal{C}$ by $\mathbf{SE}$. We observe the following simple result by considering the degrees of x and y of $W_{\mathcal{C}}(x, y)$.

$$W_{\mathcal{C}}(1, i) = |\mathbf{DE}| - |\mathbf{SE}|, \tag{1}$$

where i is the complex number such that $i^2 = -1$ and $|S|$ is the size of S.

Proposition 2.1. *Any f.s.d. even binary code $\mathcal{C}$ of length n not divisible by 8 is balanced.*

Proof. We note that for a f.s.d. even binary code $\mathcal{C}$ of length n not divisible by 8,

$$W_{\mathcal{C}}(1, i) = 0,$$

since W_1 appears in any term of $W_{\mathcal{C}}(x, y)$. Hence the claim follows from (1). □

This proposition proves that any f.s.d. even binary code of length $n \equiv 4 \pmod 8$ is balanced, which was mentioned in [9, p. 83] without a proof.

Let $\mathcal{C}$ be an $[n, n/2, d^* = 2\lfloor n/8 \rfloor]$ near-extremal f.s.d. even code with $8 \mid n$. Then the weight enumerator of $\mathcal{C}$ has the following form.

$$W_{\mathcal{C}}(x, y) = W_1^{n/2} + \cdots + \alpha W_2^{n/8} = x^n + A_{d^*} x^{n-d^*} y^{d^*} + \cdots . \tag{2}$$

As the minimum weight d^* of $\mathcal{C}$ is 2 less than the extremal minimum weight, we know that there must be one parameter in $W_{\mathcal{C}}(x, y)$. This parameter turns out to be the coefficient of $W_2^{n/8}$, α, by considering the degrees of x and y from the second equality in (2). By substituting $x = 1$ and $y = i$ into (2), we get

$$W_{\mathcal{C}}(1, i) = \alpha(-4)^{n/8}.$$

Hence by the above observation

$$|\mathbf{DE}| - |\mathbf{SE}| = (-1)^{n/8} \alpha 2^{n/4}.$$

So

$$|\mathbf{DE}| = |\mathbf{SE}| \text{ if and only if } \alpha = 0. \tag{3}$$

Lemma 2.2. *([6]) If $\mathcal{C}$ is f.s.d. even of length $n \geq 32$ and minimum weight d, then $d \leq 2\lfloor n/8 \rfloor$.*

This lemma is due to results from [3] and the fact that for n large enough there are negative numbers in the weight distributions of extremal f.s.d. even codes of length n.

As it is well known [5] that the highest minimum weights of Type I self-dual codes of lengths 8, 16, or 24 are 2, 4, or 6, respectively, and there is only one code meeting this bound, the Type I self-dual codes of these lengths with the highest minimum weights have a unique weight distribution. Generally we have the following with the help of (3).

Proposition 2.3. *The weight distribution of a near-extremal f.s.d. even code of length n with $8 \mid n$ and $|\mathbf{DE}| = |\mathbf{SE}|$ is unique and is given by (2) with $\alpha = 0$.*

This gives an elementary explanation of the fact that the weight distribution of the three Type I self-dual $[32, 16, 8]$ codes is unique [4].

Let $\mathcal{C}$ be an even binary $[n, k]$ code. The *hull* of $\mathcal{C}$, $\mathcal{C} \cap \mathcal{C}^{\perp}$, is denoted by Hull($\mathcal{C}$) and the *radical* of $\mathcal{C}$, the largest doubly-even subcode of Hull($\mathcal{C}$), is denoted by Rad($\mathcal{C}$). Clearly Rad($\mathcal{C}$)=$\mathcal{C}$ if and only if $\mathcal{C}$ is doubly-even. Rad($\mathcal{C}$) has codimension one in $\mathcal{C}$ if and only if $\mathcal{C}$ is singly-even and self-orthogonal. The only situation where Rad($\mathcal{C}$) $\neq$ Hull($\mathcal{C}$) is when $|\mathbf{DE}| = |\mathbf{SE}|$, i.e., the odd anisotropic case, the only case where $k - r$ is odd [2],[9],[11], where r is the dimension of Rad($\mathcal{C}$). In this case, a near-extremal f.s.d. even code of length n with $8 \mid n$ has $\alpha = 0$ in (2) by (3).

Suppose $\alpha \neq 0$ in (2). Then

$$n/2 = r + 2m,$$

where r = dimRad($\mathcal{C}$) = dimHull($\mathcal{C}$) [11, Theorem 2]. Note that $r \neq 0$ since $\mathbf{1} \in$ Rad($\mathcal{C}$). We also have either $|\mathbf{DE}| = 2^r(2^{2m-1} + 2^{m-1})$ and $|\mathbf{SE}| = 2^r(2^{2m-1} - 2^{m-1})$ [11, Theorem 5] or vice versa [11, pp. 287]. Therefore,

$$|\mathbf{DE}| - |\mathbf{SE}| = \pm\, 2^{r+m} = (-1)^{n/8}\alpha 2^{n/4}.$$

As $n/4 = r/2 + m$, $\alpha = \pm\, 2^{r/2}$. Hence we have the following theorem.

Theorem 2.4. *Let $\mathcal{C}$ be a near-extremal f.s.d. even (not Type II) binary $[n, n/2, 2\lfloor n/8 \rfloor]$ code and let $8 \mid n$. Then*

$$|\mathbf{DE}| = 2^{n/2-1} + \alpha 2^{n/4-1} \text{ and } |\mathbf{SE}| = 2^{n/2-1} - \alpha 2^{n/4-1},$$

where $\alpha = 0, 2^{r/2}$, or $-2^{r/2}$, where $r = dim Rad(\mathcal{C})$. Hence α must be either 0 or $\pm\, 2^i$ for $i = 1, \cdots, n/4 - 1$. When $\alpha \neq 0$, $r = 2i$ for $i = 1, \cdots, n/4 - 1$. When $\alpha = 0$, r is odd, more precisely, if $r = \frac{n}{2} - 1$ then $\mathcal{C}$ is Type I; if $r < \frac{n}{2} - 1$ then $\mathcal{C}$ is f.s.d. even and not Type I.

If $\mathcal{C}$ is a self-dual Type I $[n, n/2, 2\lfloor n/8 \rfloor]$ code, α must be 0. If $\alpha = 0$, $\mathcal{C}$ may be self-dual or not. Using Theorem 2.4 we can restrict weight enumerators of near-extremal f.s.d. even codes of lengths divisible by 8 as the following examples show.

Example 2.5. Let $8 \mid n$. The possible weight enumerator W_n of a near-extremal f.s.d. even code of length $n = 16, 24, 32$, or 40 is as follows [7]. We correct the weight enumerators W_{16} and W_{40} in [7] in the following.

$$\begin{aligned}
W_{16} &= 1 + (12 + \alpha)y^4 + (64 - 4\alpha)y^6 + (102 + 6\alpha)y^8 + \cdots, \\
W_{24} &= 1 + (64 + \alpha)y^6 + (375 - 6\alpha)y^8 + \cdots, \\
W_{32} &= 1 + (364 + \alpha)y^8 + (2048 - 8\alpha)y^{10} + \cdots, \\
W_{40} &= 1 + (2164 + \alpha)y^{10} + (10470 - 10\alpha)y^{12} + \cdots,
\end{aligned}$$

where α is as in (2).

For length 16 there exist codes with $\alpha = -8, -4, 2, 4, 8$ from Table 7 of [7]. There is no explanation in [7] about why α is always a power of 2. The reason follows immediately from Theorem 2.4 since it shows that α must be a power of 2 ranging from -2^3 to 2^3 or 0. Moreover we easily see from Theorem 2.4 that dimRad for these codes is 6, 4, 2, 4, 6, respectively. We remark that the codes $C_{16,5}$ and $C_{16,6}$ in Table 7 of [7] are *Type II self-dual* codes since $\alpha = 16$ implies that dimRad of these codes is 8. See also [1] for codes with $\alpha = 0$ and -2. There is a similar discussion about near-extremal f.s.d. even codes of length 16 [9, p. 84].

For length 24 there exist codes with $\alpha = -16, -4, 0, 2, 8, 32$ by explicitly constructing such codes [7]. Again it follows from Theorem 2.4 that α must be a power of 2 ranging from -2^5 to 2^5 or 0 and that dimRad for these codes is 8, 4, odd, 2, 6, 10, respectively. Further when dimRad is odd, we explicitly computed dimRad = 7. So their code with $\alpha = 0$ is not self-dual. Note that there exists the Type I self-dual $[24, 12, 6]$ code of length 24 with $\alpha = 0$ and dimRad = 11. Recent constructions [8] have shown that f.s.d. even codes exist for all possible α, that is α a power of 2 from -2^5 to 2^5. Further [8] codes $\mathcal{C}$ have been constructed with $\alpha = 0$ and $\mathrm{dimRad}(\mathcal{C}) = 3, 5, 7$ and 9.

Likewise for length 32 we see that α is a power of 2 ranging from -2^7 to 2^7 or 0. It is known [7] that there exist codes of length 32 with $\alpha = -64, -16, -8, -4, 4, 8, 16, 128$. In these cases, dimRad is $12, 8, 6, 4, 4, 6, 8, 14$, respectively. Also there exist the three Type I self-dual $[32, 16, 8]$ codes of length 32 with $\alpha = 0$ and dimRad = 15. Also at this length recent constructions [8] found codes for all the remaining possible α as well as $\alpha = 0$ with dimRad $= 1, 3$ and 5. Hence at length 32, f.s.d. even codes exist for all α a power of 2 from -2^7 to 2^7 or 0.

It is an open problem whether there exists a f.s.d. even $[40, 20, 10]$ code with W_{40} although there is no self-dual $[40, 20, 10]$ code. There is no f.s.d. even $[40, 20, 10]$ code with $\alpha = \pm\, 2^9$ as its radical must be a $[40, 18, 12]$ code which does not exist by [3]. It is not even known whether there exists a linear $[40, 20, 10]$ code [3].

Although there is no [48,24,12] Type 1 code [12], it is not known whether there exists a near-extremal f.s.d. even $[48, 24, 12]$ code which is not Type II. Further the existence of near-extremal f.s.d. even $[56, 28, 14]$, $[64, 32, 16]$ codes is open. There is no $[56, 28, 14]$ f.s.d. even code with $\alpha = \pm\, 2^{13}$ as its radical must be a $[56, 26, 16]$ code which does not exist by [3]. Also we know that there is no linear $[72, 36, 18]$ code by Brouwer's table [3]. We conjecture the following.

Conjecture 2.6. *There does not exist a near-extremal f.s.d. even code of length* $n \geq 48$ *with* $8 \mid n$.

Remark 2.7. This conjecture is true for Type I codes of length $n \geq 48$ with $8 \mid n$ as they must satisfy the Type II bound for $n > 48$ [12].

Acknowledgement The authors would like to thank T. Aaron Gulliver for sending a copy of [8].

References

[1] K. Betsumiya and M. Harada, Classification of formally self-dual even codes of length up to 16, *Designs, Codes, and Cryptography,* **23** (2001), 325–332.

[2] A.E. Brouwer, The linear programming bound for binary linear codes, *IEEE Trans. Inform. Theory* **39** (1993), 677–680.

[3] A.E. Brouwer, Bounds on the minimum distance of linear codes, online data at http://www.win.tue.nl/˜ aeb/voorlincod.html.

[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* **36** (1990), 1319–1333.

[5] J.H. Conway and V. Pless, and N.J.A. Sloane, The binary self-dual codes of length up to 32: A revised enumeration, *J. Combin. Theory Ser. A* **60** (1992), 183–195.

[6] J.E. Fields, P. Gaborit, W.C. Huffman, and V. Pless, On the classification of formally self-dual codes, *Proceedings of the 36th Allerton Conference on Communication, Control and Computing,* UIUC, Oct. 1998, 566–575.

[7] T.A. Gulliver and M. Harada, Classification of extremal double circulant formally self-dual even codes, *Des. Codes and Cryptogr.* **11** (1997), 25–35.

[8] T.A. Gulliver, M. Harada, T. Nishimura, and P.R.J. Östergård, Near-extremal formally self-dual even codes of lengths 24 and 32, to appear in *Des. Codes and Cryptogr.*

[9] G.T. Kennedy, Weight distributions of linear codes and the Gleason-Pierce theorem, *J. Combin. Theory Ser. A* **67** (1994), 72–88.

[10] G.T. Kennedy and V. Pless, On designs and formally self-dual codes, *Des. Codes and Cryptogr.* **4** (1994), 43–55.

[11] V. Pless, Parents, children, neighbors and the shadow, Finite fields: theory, applications, and algorithms (Las Vega, NV, 1993), *in* "Contemporary Mathematics", **168** Amer. Math. Soc., Providence, RI, 1994, 279–290.

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

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

[14] N.J.A. Sloane, Self-dual codes and lattices, Relations Between Combinatorics and Other Parts of Mathematics, *in* Proc. Symp. Pure Math. vol 34, Amer. Math. Soc., Providence, RI (1979) 273–308.

[15] H.N. Ward, Quadratic residue codes and divisibility, *in* "Handbook of Coding Theory", V.S. Pless and W.C. Huffman, Eds. Amsterdam. The Netherlands: Elsevier, 1998.