5-designs related to binary extremal self-dual codes of length $24m$

Javier de la Cruz and Wolfgang Willems

Otto-von-Guericke Universität, Magdeburg, Germany
Universidad del Norte, Barranquilla, Colombia

Abstract

We prove that the binary code C of length 120 related to a self-orthogonal 5-$(120, 24, 8855)$ design is self-dual and has minimum distance $d = 24$ (i.e. C is extremal) or $d = 16$.

Keywords: *Extremal self-dual codes,* 5-*designs*

1 Introduction

A t-(v, k, λ) design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, shortly a t-design, is a set $\mathcal{P}$ of v points together with a collection $\mathcal{B}$ of k-subsets B of $\mathcal{P}$ (called blocks) such that every t distinct points are together incident with exactly λ blocks. The design is called self-orthogonal if

$$|B \cap B'| \equiv k \bmod 2$$

for all blocks $B, B' \in \mathcal{B}$.

Let C be a binary extremal self-dual code of length $n = 24m$. According to Mallows and Sloane [12], the minimum distance of an extremal code of length $24m$ satisfies $d = 4m+4$. We put $\mathcal{P} = \{1, \ldots, 24m\}$ and define the blocks $B \in \mathcal{B}$ as supports of codewords of minimal weight. Thus the block size equals $4m + 4$. Due to Assmus and Mattson [1], $\mathcal{D}_C = (\mathcal{P}, \mathcal{B})$ forms a self-orthogonal 5-$(24m, 4m + 4, \lambda)$ design.

If A_d denotes the number of codewords of minimal weight a double counting argument shows that

$$\binom{n}{5}\lambda = A_d\binom{d}{5}.$$

Since, according to [12],

$$A_d = \frac{\binom{n}{5}\binom{5m-2}{m-1}}{\binom{d}{5}}$$

we obtain

$$\lambda = \binom{5m-2}{m-1}.$$

Thus a binary extremal self-dual code of length $n = 24m$ yields a self-orthogonal

$$5\text{-}(24m, 4m+4, \binom{5m-2}{m-1})$$

design.

Conversely, suppose that $\mathcal{D}$ is a self-orthogonal 5-$(24m, 4m+4, \binom{5m-2}{m-1})$ design. The related binary code $C(\mathcal{D})$ is defined as the $\mathbb{F}_2$-linear span of the rows of the block-point incidence matrix of $\mathcal{D}$. Clearly, $C(\mathcal{D})$ is self-orthogonal since $\mathcal{D}$ is self-orthogonal.

In order to prove that $C(\mathcal{D})$ is self-dual we may proceed as follows. Let $c^\perp \in C(\mathcal{D})^\perp$ with $\mathrm{wt}(c^\perp) = w$ and let S denote the support of $c^\perp$. Hence $|S| = w$. If n_i denotes the number of blocks intersecting S in exactly i points (the n_i are usually called intersection numbers) and

$$\lambda_j = \lambda \frac{\binom{24m-j}{5-j}}{\binom{4m+4-j}{5-j}} \tag{1}$$

then we have the Mendelsohn equations

$$\sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} \binom{2i}{j} n_{2i} = \lambda_j \binom{w}{j} \qquad (j = 0, 1, \ldots, 5) \tag{2}$$

(see [13] or ([3], Satz 2.1.1). In case we are able to prove that the system (2) of linear equations has nonnegative integer solutions $n_{2i} \in \mathbb{N}_0$ only if $4 \mid w$ then $C(\mathcal{D})^\perp$ is doubly-even which implies

$$C(\mathcal{D})^\perp \subseteq (C(\mathcal{D})^\perp)^\perp = C(\mathcal{D}).$$

Hence $C(\mathcal{D})$ is self-dual since $C(\mathcal{D}) \subseteq C(\mathcal{D})^\perp$.

This approach works properly for $m = 1, \ldots, 25$ unless $m = 7, 13, 14, 15$ and 23. In the exceptional cases the method fails since there might be solutions $n_{2i} \in \mathbb{N}_0$ of (2) for all $w \equiv 2 \bmod 4$.

Remark 1 Note that for $m = 1$ there is exactly one binary extremal self-dual code, namely the $[24, 12, 8]$ extended Golay code and exactly one 5-$(24, 8, 1)$ design, a Steiner system, where the related code is the binary extended Golay code (see ([14], Theorem 5) and ([2], Theorem 8.6.2)). For $m = 2$ there is again exactly one binary extremal self-dual code, namely the binary extended quadratic residue code [10] and exactly one self-orthogonal 5-$(48, 12, 8)$ design ([9], Theorem 1.1), where the related code is the binary extended quadratic residue code of length 48.

In case $m = 3$ and $m = 4$ we do not know about the existence neither of binary extremal self-dual codes of length 72 or 96 nor of self-orthogonal 5-$(72, 16, 78)$ or 5-$(96, 20, 816)$ designs $\mathcal{D}$. However, according to [8] and [7], the related codes $C(\mathcal{D})$ of the putative designs are extremal self-dual in both cases.

2 The case $m = 5$

Unfortunately, for $m = 5$, we are not able to prove that the related code of the putative 5-design is extremal. More precisely, we have

Theorem Let $\mathcal{D}$ be a self-orthogonal 5-$(120, 24, 8855)$ design. Then $C(\mathcal{D}) = C(\mathcal{D})^{\perp}$ with minimum distance $d = 16$ or $d = 24$.

Proof: Let $\mathcal{D}$ be a self-orthogonal 5-$(120, 24, 8855)$ design. According to (1) one easily computes $\lambda_0 = 39703755$, $\lambda_1 = 7940751$, $\lambda_2 = 1534767$, $\lambda_3 = 286143$, $\lambda_4 = 51359$ and $\lambda = \lambda_5 = 8855$. Let $C = C(\mathcal{D})$. Clearly $C \subseteq C^{\perp}$ since $\mathcal{D}$ is self-orthogonal.

Next let $c^{\perp} \in C^{\perp}$ with $\mathrm{wt}(c^{\perp}) = w > 0$. Since $n_{2i} = 0$ for $2i > 24$ the system (2) of equations may be written as

$$xA = b \tag{3}$$

where

$$x = (n_0,\, n_2,\, n_4,\, n_6,\, n_8,\, n_{10},\, n_{12},\, n_{14},\, n_{16},\, n_{18},\, n_{20},\, n_{22},\, n_{24}),$$

$$b = \left(\ \lambda_0,\quad \lambda_1\tbinom{w}{1},\quad \lambda_2\tbinom{w}{2},\quad \lambda_3\tbinom{w}{3},\quad \lambda_4\tbinom{w}{4},\quad \lambda_5\tbinom{w}{5}\ \right)$$

and

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 \\ 1 & 4 & 6 & 4 & 1 & 0 \\ 1 & 6 & 15 & 20 & 15 & 6 \\ 1 & 8 & 28 & 56 & 70 & 56 \\ 1 & 10 & 45 & 120 & 210 & 252 \\ 1 & 12 & 66 & 220 & 495 & 792 \\ 1 & 14 & 91 & 364 & 1001 & 2002 \\ 1 & 16 & 120 & 560 & 1820 & 4368 \\ 1 & 18 & 153 & 816 & 3060 & 8568 \\ 1 & 20 & 190 & 1140 & 4845 & 15504 \\ 1 & 22 & 231 & 1540 & 7315 & 26334 \\ 1 & 24 & 276 & 2024 & 10626 & 42504 \end{pmatrix}.$$

Solving the system (3) of equations we find

$$n_{10} = \beta_{10} - 6n_{12} - 21n_{14} - 56n_{16} - 126n_{18} - 252n_{20} - 462n_{22} - 792n_{24},$$

where

$$\beta_{10} = \frac{1}{32 \cdot 8 \cdot 3}(1771w^5 - 120428w^4 + 3253580w^3 - 41174416w^2 + 204795264w).$$

One easily checks that $\beta_{10} \notin \mathbb{Z}$ if $w \not\equiv 0 \bmod 4$. Therefore $w \equiv 0 \bmod 4$ which shows that $C^{\perp}$ is doubly-even. In particular, $C^{\perp}$ is self-orthogonal which proves that C is self-dual.

Finally, in order to compute the minimum distance d of C let $c \in C^{\perp} = C$ be of minimum weight $\mathrm{wt}(c) = w = d$. According to (2) we have

$$2\sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} \binom{2i}{2} n_{2i} - \sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} 2in_{2i} = 2\lambda_2 \binom{w}{2} - \lambda_1 w,$$

hence

$$\sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} 2i(2i-2)n_{2i} = w((w-1)\lambda_2 - \lambda_1).$$

Since $2i(2i-2)n_{2i} \geq 0$ for $i = 0, ..., \lfloor \frac{w}{2} \rfloor$ we obtain $w \geq \frac{\lambda_1 + \lambda_2}{\lambda_2} > 6$. Therefore the minimum distance d satisfies $d \geq 8$.

Using a computer algebra system we see that for $w = 8$ and $w = 12$ the system (3) of equations has no solution consisting of nonnegative integers. Thus we have $d \geq 16$. In contrast to $w = 8$ and $w = 12$ there are nonnegative integer solutions for $w = 16$ and $w = 20$, for instance

$$x = (1599377, 17248920, 16427320, 4325776, 66690, 35672, 0, 0, 0, 0, 0, 0)$$

and

$$x = (574140, 10214100, 18892755, 8752800, 1200300, 69660, 0, 0, 0, 0, 0, 0),$$

respectively. We claim that $d = 20$ can not occur which finishes the proof.

By Gleason's theorem [6], the homogenous weight enumerator $W_C(x, y)$ is given by

$$W_C(x,y) = \sum_{i=0}^{5} a_i (x^8 + 14x^4y^4 + y^8)^{15-3i}(x^4y^4(x^4 - y^4)^4)^i,$$

where $a_i \in \mathbb{Z}$ for $i = 0, ..., 5$. Thus

$$\begin{aligned} W_C(1,y) &= a_0 + (210a_0 + a_1)y^4 + (20595a_0 + 164a_1 + a_2)y^8 + \dots \\ &= A_0 + A_{20}y^{20} + A_{24}y^{24} + \dots, \end{aligned}$$

where A_i denotes the number of codewords of weight i. In particular we have

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 210 & 1 & 0 & 0 & 0 \\ 20595 & 164 & 1 & 0 & 0 \\ 1251460 & 12282 & 118 & 1 & 0 \\ 52705485 & 554740 & 6085 & 72 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

The unique solution of this system of equations is

$$(a_0, a_1, a_2, a_3, a_4) = (1, -20, 13845, -305950, 1571490).$$

Therefore $A_{20} = 492372 + a_5 > 0$ and $A_{24} = 29856315 - 20a_5$. Since $-a_5 < 492372$ we get

$$A_{24} = 29856315 - 20a_5 < 29856315 + 9847440 = 39703755$$

which contradicts the fact that the incidence matrix of the design $\mathcal{D}$ has 39703755 row vectors of weight 24. □

In the proof we used only the Mendelsohn equations from design theory. There are other equations like the Köhler equations or higher intersection numbers (see [3]). However neither of them lead to a contradiction in case $d = 16$.

3 Automorphism groups

It is well-known that the automorphism group of the binary extended Golay code coincides with the automorphism group of its related 5-$(24, 8, 1)$ design; it is the Mathieu group M_{24}. The same happens with the binary extended quadratic residue code of length 48 and its related self-orthogonal 5-$(48, 12, 8)$ design. The group is PSL$(2, 47)$. In general we have

Proposition 2 *Let C be a binary extremal self-dual $[24m, 12m, 4m + 4]$ code with related self-orthogonal 5-$(24m, 4m + 4, \binom{5m-2}{m-1})$ design $\mathcal{D}$. If $C(\mathcal{D})^{\perp} = C(\mathcal{D})$ then*

$$\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D}).$$

Proof: The condition $C(\mathcal{D})^{\perp} = C(\mathcal{D})$ implies in particular that C is generated by the set $S = \{v_1, \ldots, v_s\}$ of all codewords of minimum weight $w = d = 4m + 4$.
Let $\sigma \in \mathrm{Aut}(\mathcal{D})$. For $c = \sum_{i=1}^{s} \alpha_i v_i \in C$ we put $\sigma(c) = \sum_{i=1}^{s} \alpha_i \sigma(v_i)$. Note that this is well defined since σ permutes the coordinates $\{1, \ldots, 24m\}$. Clearly, $\sigma(v_i) \in S \subseteq C$ for all i, hence $\sigma(c) \in C$. This proves that $\sigma \in \mathrm{Aut}(C)$.
Conversely, suppose that $\sigma \in \mathrm{Aut}(C)$. Since σ acts as a permutation on S it induces a permutation on the blocks which shows that $\sigma \in \mathrm{Aut}(\mathcal{D})$. □

Remarks 3 a) By the Theorem and the computations we mentioned in the previous sections we have $C(\mathcal{D})^{\perp} = C(\mathcal{D})$ for all self-orthogonal 5-$(24m, 4m + 4, \binom{5m-2}{m-1})$ designs $\mathcal{D}$ with $m = 1, \ldots, 25$ unless $m = 7, 13, 14, 15, 23$. Thus for these m the automorphism group of a binary extremal self-dual $[24m, 12m, 4m + 4]$ code C is equal to the automorphism group of its related design $\mathcal{D}$.
b) Since $C(\mathcal{D})$ is extremal for $m = 3$ and $m = 4$ the automorphism group of a self-orthogonal 5-$(72, 16, 78)$ or 5-$(96, 20, 816)$ design equals the automorphism group of the related extremal self-dual code. Thus, according to the main theorem in [4], the automorphism group of a putative self-orthogonal 5-$(72, 16, 78)$ design is solvable of order less or equal to 36. Information on the automorphism group of a self-orthogonal 5-$(96, 20, 816)$ design can be taken from [5].

4 Questions

Let $\mathcal{D}$ be a self-orthogonal 5-$(24m, 4m+4, \binom{5m-2}{m-1})$ design and let $C(\mathcal{D})$ denote its related code as defined in the introduction. Due to the results in the literature and the previous sections we may ask.

Question 1 Do we always have $C(\mathcal{D})^{\perp} = C(\mathcal{D})$?

Question 2 Is $C(\mathcal{D})$ always an extremal self-dual $[24m, 12m, 4m+4]$ code?

Note, that an affirmative answer to the question 1 implies that the automorphism group of an extremal self-dual code of length $24m$ is equal to the automorphism group of its related 5-design. An affirmative answer of question 2 says that the existence of an extremal self-dual $[24m, 12m, 4m+4]$ code is equivalent to the existence of a self-orthogonal 5-$(24m, 4m+4, \binom{5m-2}{m-1})$ design.

References

[1] E.F. Assmus, Jr. and H.F. Mattson Jr., New 5-designs. *J. Combin. Theory* **6** (1969), 122-151.

[2] E.F. Assmus, Jr. and J.D. Key, *Designs and their Codes.* Cambridge University Press 1992

[3] A. Betten, Schnittzahlen von Designs, Bayreuther Mathematische Schriften, Heft 58, 2000.

[4] E.A. O'Brien and W. Willems, On the automorphism group of a binary self-dual doubly-even [72,36,16] code. To appear *IEEE Trans. Inform. Theory.*

[5] J. de la Cruz and W. Willems, On extremal self-dual codes of length 96. To appear *IEEE Trans. Inform. Theory.*

[6] A.M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, in *Actes Congrès Internat. Math.* **3** (1970), 211-215.

[7] M. Harada, Remark on a 5-design related ton a putative extremal doubly-even self-dual $[96, 48, 20]$ code. *Designs, Codes and Cryptography* **37** (2005), 355-358.

[8] M. Harada, M. Kitazume and A. Munemasa, On a 5-design related to an extremal doubly-even self-dual code of length 72. *J. Combin. Theory, Series A* **107** (2004), 143-146.

[9] M. Harada, A. Munemasa and V.D. Tonchev, A characterization of designs related to an extremal doubly-even self-dual code of length 48. *Annals of Combinatorics* **5** (2005), 189-198.

[10] S.K. Houghten, C.W.H. Lam, L.H. Thiel and J.A. Parker, The extended quadratic residue code is the only $(48, 24, 12)$ self-dual doubly-even code. *IEEE Trans. Inform. Theory* **49** (2003), 53-59.

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

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

[13] N.S. Mendelsohn, Intersection numbers of t-designs. In: Studies in Pure Mathematics (presented to Richard Rado), Academic Press, London 1971, 145-150.

[14] V. Pless, On the uniqueness of the Golay codes. *J. Comb. Theory* **5** (1968), 215-228.