Self-orthogonal designs

Akihiro Munemasa
(joint work with Masaaki Harada and Tsuyoshi Miezaki)

June 22, 2015
The 32nd Algebraic Combinatorics Symposium
Kanazawa

Definition 1. A t-(v,k,λ) design is a pair $(X,\mathcal{B})$, where

- X is a finite set, $|X| = v$,
- $\mathcal{B} \subset \binom{X}{k} = \{k\text{-element subsets of } X\}$,
- $\forall T \in \binom{X}{t}$,
$$\lambda = |\{B \in \mathcal{B} \mid B \supset T\}|.$$

Elements of X are called "points", elements of $\mathcal{B}$ are called "blocks". According to [3], the existence of a 3-$(16,7,5)$ design is unknown. Recently, Nakić [4] showed that such a design cannot have an automorphism of order 3. In this talk, we give constructions of 3-$(16,8,3\mu)$ designs for $1 \le \mu \le 5$.

Definition 2. A design $(X,\mathcal{B})$ is *self-orthogonal* if

$$|B \cap B'| \equiv 0 \pmod 2 \quad (\forall B, B' \in \mathcal{B}).$$

In particular, in a self-orthogonal design, $k \equiv 0 \pmod 2$ holds. Let M be the block-point incidence matrix. Then

$$\text{self-orthogonal} \iff MM^\top = 0 \text{ over } \mathbb{F}_2.$$

We call the row space C of M the code of the design. Then $C \subset C^\perp$.

Example 1. The row space of the matrix $\begin{bmatrix} I_4 & J_4 - I_4 \end{bmatrix}$ over $\mathbb{F}_2 = \{0,1\}$ contains 14 vectors of weight 4, forming a self-orthogonal 3-$(8,4,1)$ design.

More generally, if H is a Hadamard matrix of order $8n$, i.e., H is a $8n \times 8n$ matrix with entries in $\{\pm 1\}$ satisfying $HH^\top = 8nI$, then one obtains a self-orthogonal 3-$(8n, 4n, 2n-1)$ design.

Fundamental problem in combinatorial design theory is:

Problem 1. Given t, v, k, λ, does there exist a t-(v, k, λ) design?

The main interest was to show that t-design exists for an arbitrary large t. Before Teirlinck [9] showed that this is the case in 1987, only a few t-designs with $t \geq 5$ were known. We suspect that, however, self-orthogonal designs are very restricted subclass of designs, the corresponding problem might have an opposite answer.

Note that the 5-$(24, 8, 1)$ design by Witt [11] is self-orthogonal, and the Assmus-Mattson theorem [1] gives why one obtains a 5-design: every extremal binary self-dual code of length multiple of 24 gives 5-designs. In our work we only consider orthogonality mod 2. For example, the 5-$(12, 6, 1)$ design of Witt [11] is not self-orthogonal. It is, however, self-orthogonal in some other sense.

The Assmus–Mattson theorem [1] implies that every binary doubly even self-dual $[24m, 12m, 4m+4]$ code supports a 5-$(24m, 4m+4, \lambda)$ design.

- $m = 1$: Witt design; related designs were characterized by Tonchev [10].
- $m = 2$: Harada–Munemasa–Tonchev [7].

For $m \geq 3$, existence is unknown:

- $m = 3$ by Harada–Munemasa–Kitazume [6], $m = 4$ by Harada [5], $m \geq 5$ by de la Cruz and Willems [2].

For a systematic study for a more general case, we refer Lalaude-Labayle [8]. In this talk, however, instead of considering the problem:

> given a self-dual code C of length v and minimum weight k, what is the maximum t such that
>
> $$\mathcal{B} = \{\text{supp}(x) \mid x \in C,\ \text{wt}(x) = k\}$$
>
> is a t-design?

we take a design-theoretic viewpoint and aim for a classification of designs, not of codes. This problem is more general in the following sense. Let C be the code of a self-orthogonal design. Identifying subsets with their characteristic vectors, we have

$$\mathcal{B} \subset \{x \in C \mid \mathrm{wt}(x) = k\} \subset C \subset C^{\perp}, \quad 0 < k \leq \text{minimum weight of } C.$$

In the previously considered situation of Lalaude-Labayle [8],

$$\mathcal{B} = \{x \in C = C^{\perp} \mid \mathrm{wt}(x) = k\},$$

which we call "saturated".

In the unsaturated case, the situation could be different in three ways:

(i) $C \subsetneqq C^{\perp}$

(ii) $\mathcal{B} \subsetneqq \{x \in C \mid \mathrm{wt}(x) = k\}$

(iii) $k > \min\{\mathrm{wt}(x) \mid x \in C,\ x \neq 0\}$

Out main tool for the investigation is so-called the Mendelsohn equations. Let $(X, \mathcal{B})$ be a t-(v, k, λ) design, $S \subset X$.

$$n_j = |\{B \in \mathcal{B} \mid j = |B \cap S|\}|.$$

Then

$$\sum_{j \geq 1} \binom{j}{i} n_j = \lambda_i \binom{|S|}{i} \quad (i = 1, \ldots, t), \tag{1}$$

is a system of t linear equations in unknowns $n_1, n_2, \ldots$ (at most $\min\{k, |S|\}$). The number of unknowns can be reduced if

- $S \in C^{\perp}$, then $n_j = 0$ for j odd.
- $k = \min C^{\perp}$, then $n_j = 0$ for $j > k/2$.

Clearly, the dual code $C^{\perp}$ of the code C of a t-design has minimum weight at least $t + 1$. Moreover, if equality holds with $t = 3$, then we have the following consequence.

Lemma 1. If $(X, \mathcal{B})$ is a self-orthogonal 3-(v, k, λ) design, and the dual code of its code has minimum weight 4, then $v = 2k$.

Proof. There are $t = 3$ Mendelsohn equations (1) for 2 unknowns n_2, n_4. Existence of a solution gives $v = 2k$. □

We now consider self-orthogonal 3-$(2k, k, \lambda)$ designs. Recall 3-$(8, 4, 1)$ design exists, since this is nothing but the unique Hadamard 3-designs.

Note that the 5-$(12, 6, 1)$ design of Witt [11] which is 3-$(12, 6, 12)$ design is not self-orthogonal. Let $(X, \mathcal{B})$ be a 3-$(12, 6, \lambda)$ design. Divisibility implies $\lambda \equiv 0 \pmod 2$, and $|\mathcal{B}| = 11\lambda$. Moreover, if $(X, \mathcal{B})$ is self-orthogonal, then its code C is contained in the unique self-dual $[12, 6, 4]$ code which has 32 vectors of weight 6, so $\lambda \leq 2$, hence $\lambda = 2$. Since a 3-$(12, 6, 2)$ design is an extension of a symmetric 2-$(11, 5, 2)$ design, it cannot be self-orthogonal. Alternatively, Mendelsohn equations (1) with respect to a block leads to a contradiction for all λ.

Now let $(X, \mathcal{B})$ be a self-orthogonal 3-$(16, 8, \lambda)$ design. Divisibility implies $\lambda \equiv 0 \pmod 3$. The largest number of vectors of weight 8 in a self-orthogonal codes of length 16 gives an upper bound $\lambda \leq 18$.

For $\lambda = 3$, we have Hadamard 3-designs, so $(X, \mathcal{B})$ comes from the known classification of Hadamard matrices of order 16.

Theorem 1. Let $\lambda = 3\mu \geq 6$, where μ is an integer. The following are equivalent:

(i) there exists a self-orthogonal 3-$(16, 8, \lambda)$ design,

(ii) there exists an equitable partition of the folded halved 8-cube with quotient matrix
$$\begin{bmatrix} 4(\mu-1) & 4(8-\mu) \\ 4\mu & 4(7-\mu) \end{bmatrix},$$

(iii) $\mu \in \{2, 3, 4, 5\}$.

In particular, there is no self-orthogonal 3-$(16, 8, 18)$ design.

Proof. Let $(X, \mathcal{B})$ be a self-orthogonal 3-$(16, 8, \lambda)$ design, where $\lambda = 3\mu \geq 6$. Then there exists a doubly even self-dual code C containing the code of $(X, \mathcal{B})$. From the classification of doubly even self-dual codes of length 16, C has minimum weight 4. Let S be a codeword of C with weight 8. Then the Mendelsohn equations (1) give

$$(n_0, n_2, n_4, n_6, n_8) = (1, 4(\mu-1), 22\mu + 6, 4(\mu-1), 1) \text{ or } (0, 4\mu, 22\mu, 4\mu, 0).$$

In particular, $n_2 \geq 4(\mu-1) > 0$. One of the doubly even self-dual $[16,8,4]$ code, i.e., $e_8 \oplus e_8$ cannot be C, since there exists a codeword x of weight 8 in C such that $|\operatorname{supp}(x) \cap \operatorname{supp}(y)| \neq 2$ for any codeword y of weight 8 in C. This is impossible since $n_2 > 0$ as shown above.

Now we conclude that C is isomorphic to the other doubly even self-dual $[16,8,4]$ code, d_{16}. The following gives a construction of a 3-$(16,8,12)$ design. Let $\mathcal{P} = \{1,\dots,16\}$, and

$$X = \{\{\operatorname{supp}(x), \mathcal{P} \setminus \operatorname{supp}(x)\} \mid x \in C,\ \operatorname{wt}(x) = 8\}.$$

Then $|X| = 99$. Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be the orbits of length 35 and 64, respectively, on X under $\operatorname{Aut} C$. Suppose that $(\mathcal{P}, \mathcal{B})$ is a 3-$(16,8,3\mu)$ design. Set

$$\overline{\mathcal{B}} = \{\{B, \mathcal{P} \setminus B\} \mid B \in \mathcal{B}\},$$
$$\overline{\mathcal{B}}_i = \overline{\mathcal{B}} \cap \mathcal{O}_i \quad (i = 1, 2).$$

We define a graph $\Gamma = (X, E)$, where E consists of pairs $\{\{B_1, \mathcal{P}\setminus B_1\}, \{B_2, \mathcal{P}\setminus B_2\}\}$ such that $|B_1 \cap B_2| \in \{2, 6\}$. Then Γ has two connected components $\mathcal{O}_1$ and $\mathcal{O}_2$. The induced subgraphs on $\mathcal{O}_1$ and $\mathcal{O}_2$ are regular of valency 16 and 28, respectively. From the solution of the Mendelsohn equations, we see that $\mathcal{O}_i$ admits an equitable partition $\overline{\mathcal{B}}_i \cup (\mathcal{O}_i \setminus \overline{\mathcal{B}}_i)$ whose collapsed adjacency matrices are

$$\begin{bmatrix} 4(\mu-1) & 4(5-\mu) \\ 4\mu & 4(4-\mu) \end{bmatrix}, \tag{2}$$

$$\begin{bmatrix} 4(\mu-1) & 4(8-\mu) \\ 4\mu & 4(7-\mu) \end{bmatrix}, \tag{3}$$

respectively. Moreover, we have

$$4(5-\mu)|\overline{\mathcal{B}}_1| = 4\mu(|\mathcal{O}_1| - |\overline{\mathcal{B}}_1|),$$
$$4(8-\mu)|\overline{\mathcal{B}}_2| = 4\mu(|\mathcal{O}_2| - |\overline{\mathcal{B}}_2|).$$

Thus

$$|\overline{\mathcal{B}}_1| = 7\mu,$$
$$|\overline{\mathcal{B}}_2| = 8\mu.$$

The induced subgraph on $\mathcal{O}_1$ is isomorphic to the Grassmann graph $J_2(4,2)$, and an equitable partition with quotient matrix (2) exists. Indeed, for $\mu = 1$, it is simply the set of all lines through a point in $PG(3,2)$. For $\mu = 2$, it is the set of all lines through a point p and all lines on an plane $\pi \not\ni p$. For $\mu = 3$ and 4, we simply take the complementary set for $\mu = 2$ and 1, respectively. For $\mu = 5$, the partition is trivial. Therefore, the existence of a self-orthogonal 3-$(16, 8, 3\mu)$ design for $\mu \in \{2, 3, 4, 5\}$ is equivalent to the existence of an equitable partition of the subgraph induced by $\mathcal{O}_2$ with quotient matrix (3). It turns out that the subgraph induced by $\mathcal{O}_2$ is isomorphic to the folded halved 8-cube, and the existence of an appropriate equitable partition can be verified easily by computer. □

Comparing the solution of the Mendelsohn equations with the weight distribution of the self-dual codes of length 20 whose classification is already known, we obtain the following theorem.

Theorem 2. There is no self-orthogonal 3-$(20, 10, \lambda)$ design.

Regarding a self-orthogonal 3-$(24, 12, \lambda)$ design, the Assmus-Mattson theorem implies that there is a 5-$(24, 12, 48)$ design which is 3-$(24, 12, 280)$ design. Does there exist other self-orthogonal 3-$(24, 12, \lambda)$ designs?

References

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

[2] J. de la Cruz and W. Willems, 5-designs related to binary extremal self-dual codes of length $24m$, Theory and applications of finite fields, 75–80, Contemp. Math., 579, Amer. Math. Soc., Providence, RI, 2012.

[3] J. Dinitz and C. Colbourn, eds., The CRC Handbook of Combinatorial Designs, 2nd ed., Chapman & Hall/CRC Press, 2006.

[4] A. Nakić, Non-existence of a simple 3-$(16, 7, 5)$ design with an automorphism of order 3, Discrete Math. 338 (2015), 555–565.

[5] M. Harada, Remark on a putative extremal doubly-even self-dual code of length 96 and its 5-design, Designs, Codes and Cryptography 37 (2005), 355–358.

[6] 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, Ser. A 107 (2004), 143–146.

[7] 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 9 (2005), 189–198.

[8] M. Lalaude-Labayle, On binary linear codes supporting t-designs, IEEE Trans. Inform. Theory 47 (2001), 2249–2255.

[9] L. Teirlinck, Non-trivial t-designs without repeated blocks exist for all t, Discrete Math. 65 (1987), 301–311.

[10] V.D. Tonchev, A characterization of designs related to the Witt system $S(5, 8, 24)$, Math. Z. 191 (1986), 225–230.

[11] E. Witt, Über Steinersche systeme, Abh. Math. Sem. Univ. Hamburg. 12 (1938), 265–275.