Self-orthogonal designs

Akihiro Munemasa

Graduate School of Information Sciences
Tohoku University
(joint work with Masaaki Harada and Tsuyoshi Miezaki)

June 22, 2015
The 32nd Algebraic Combinatorics Symposium
Kanazawa

A t-(v,k,λ) design $(X,\mathcal{B})$

- 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".

Block Design for Piano

CRC Handbook of Combinatorial Designs, pp.79–80

Rephrased in terms of the 5-$(12,6,1)$ design, this means:

There are 12 notes, distributed into 6-note arpeggios, in such a way that every combination of 5 particular notes comes together exactly once.

The pianist does not play all the $\binom{12}{6} = 924$ combinations; only 132 arpeggios.

Self-orthogonal designs

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 $k \equiv 0 \pmod 2$.

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 (binary) code of the design. Then $C \subset C^\perp$.

Hadamard designs

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
$HH^\top = 8nI$,
$\implies$ a self-orthogonal 3-$(8n, 4n, 2n - 1)$ design.

Existence problem

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

Before Teirlinck (1987), only a few t-designs with $t \geq 5$ were known.

The 5-$(24, 8, 1)$ design by Witt (1938) is self-orthogonal.
Assmus-Mattson theorem (1969) gives a reason: extremal binary self-dual code $\rightarrow$ 5-designs.

In our work we only consider orthogonality mod 2. The 5-$(12, 6, 1)$ design of Witt (1938) is not self-orthogonal.

5-designs from binary self-dual codes

$[24m, 12m, 4m + 4]$ code $\to$ 5-$(24m, 4m + 4, \lambda)$ design.

- $m = 1$: Witt design; related designs were characterized by Tonchev (1986)
- $m = 2$: Harada-M.-Tonchev (2005)

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

- $m = 3$ by Harada-M.-Kitazume (2004), $m = 4$ by Harada (2005), $m \geq 5$ by de la Cruz and Willems (2012).

For a systematic study:

- Lalaude-Labayle (2001)
- A.M., RIMS talk (2005)

Design theoretic viewpoint

Instead of considering the problem: "given a self-dual code C of length v and k, what is the maximum t such that

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

is a t-design?",

let C be the code of a self-orthogonal design. Then

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

In the previously considered situation

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

"saturated".

$C =$ the code of a design $(X, \mathcal{B})$

Suppose $(X, \mathcal{B})$ is self-orthogonal, i.e., $C \subset C^\perp$. Unsaturated case:

1. $C \subsetneqq C^\perp$
2. $\mathcal{B} \subsetneqq \{x \in C \mid \mathrm{wt}(x) = k\}$
3. $k > \min\{\mathrm{wt}(x) \mid x \in C,\ x \neq 0\}$

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

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

a system of t linear equations in unknowns $n_1, n_2, \ldots$ (at most $\min\{k, |S|\}$).
If $S \in C^{\perp}$, then $n_j = 0$ for j odd.
If $k = \min C^{\perp}$, then $n_j = 0$ for $j > k/2$.

Dual weight 4

The dual code $C^{\perp}$ of the code C of a t-design has minimum weight at least $t+1$.

Lemma

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 for 2 unknowns n_2, n_4. □

Recall 3-$(8, 4, 1)$ design exists.

$\nexists$ self-orthogonal 3-$(12, 6, \lambda)$ design

Witt: 5-$(12, 6, 1)$ design which is 3-$(12, 6, 12)$ design (not self-orthogonal).

- Divisibility implies $\lambda \equiv 0 \pmod{2}$.
- $|\mathcal{B}| = 11\lambda$.
- C is contained in the unique self-dual $[12, 6, 4]$ code which has 32 vectors of weight 6, so $\lambda \leq 2$, hence $\lambda = 2$.
- 3-$(12, 6, 2)$ design is an extension of a symmetric 2-$(11, 5, 2)$ design, so it cannot be self-orthogonal.
- Alternatively, Mendelsohn equation w.r.t. a block leads to a contradiction for all λ.

3-$(16, 8, \lambda)$ design

- Divisibility implies $\lambda \equiv 0 \pmod 3$.
- Largest number of vectors of weight 8 in a self-orthogonal codes of length $16 \implies \lambda \leq 18$.

$\lambda = 3$: Hadamard designs.

$\lambda = 6, 9, 12, 15, 18?$

Theorem

Let $\lambda = 3\mu$. The following are equivalent:

1. $\exists$ a self-orthogonal 3-$(16, 8, \lambda)$ design,
2. $\exists$ an equitable partition of the folded halved 8-cube with quotient matrix
$$\begin{bmatrix} 4(\mu - 1) & 4(8 - \mu) \\ 4\mu & 4(7 - \mu) \end{bmatrix}.$$
3. $\mu \in \{1, 2, 3, 4, 5\}$.

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

The folded halved 8-cube

The 8-cube is the graph with vertex set $\{0,1\}^8$, two vertices are adjacent whenever they differ by exactly one coordinate.

'halved' $=$ even-weight vectors
'folded' $=$ identify with complement

The folded halved 8-cube Γ has 2^6 vertices, and it is 28-regular.

Equitable partition: $A =$ adjacency matrix of Γ,

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}, \quad A_{ij}\mathbf{1} = q_{ij}\mathbf{1}, \quad Q = (q_{ij}).$$

Theorem

Let $\lambda = 3\mu$. The following are equivalent:

1. $\exists$ a self-orthogonal 3-$(16, 8, \lambda)$ design,
2. $\exists$ an equitable partition of the folded halved 8-cube with quotient matrix

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

3. $\mu \in \{1, 2, 3, 4, 5\}$.

3-$(20, 10, \lambda)$ design

Theorem

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

Proof.

Compare the solution of the Mendelsohn equations with the weight distribution of the self-dual codes of length 20 whose classification is already known. □

3-$(24, 12, \lambda)$ design

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?