Nonexistence of a quasi-symmetric 2-(37, 9, 8) design

Akihiro Munemasa
(joint work with Masaaki Harada and Vladimir D. Tonchev)
arXiv:1606.08909

Tohoku University

November 29, 2016
Design of experiments, codes and related combinatorial structures
AkiuResort Hotel Crescent

Classification of doubly even self-dual codes

Conway and Pless, J. Combin. Theory, Ser. A (1980)

> *. . . so 17000 might be a poor lower bound. However, even this weak bound makes it clear that it would not be sensible to enumerate the [40,20] doubly even self-dual codes.*

Betsumiya, Harada and Munemasa, Elec. J. Combin. (2012)
There are

$$16470 \text{ doubly even self-dual } [40, 20, 8] \text{ codes,}$$
$$77873 \text{ doubly even self-dual } [40, 20, 4] \text{ codes.}$$

This classification was crucial in proving the nonexistence of a quasi-symmetric 2-$(37, 9, 8)$ design.

A 2-(v, k, λ) design is a pair $(\mathcal{P}, \mathcal{B})$, where

- $|\mathcal{P}| = v$, $\mathcal{B} \subset \binom{\mathcal{P}}{k}$,
- $|\{B \in \mathcal{B} \mid B \ni p, q\}| = \lambda$ for all $\{p, q\} \in \binom{\mathcal{P}}{2}$.

Write

$$b = |\mathcal{B}|, \quad r = |\{B \in \mathcal{B} \mid B \ni p\}|.$$

$$\text{symmetric if } |\{|B \cap B'| \mid B, B' \in \mathcal{B},\ B \neq B'\}| = 1,$$
$$\text{quasi-symmetric if } |\{|B \cap B'| \mid B, B' \in \mathcal{B},\ B \neq B'\}| = 2.$$

For a quasi-symmetric design, write

$$\{|B \cap B'| \mid B, B' \in \mathcal{B},\ B \neq B'\} = \{x, y\}$$

with $x < y$ (intersection numbers, uniquely determined by v, k, λ).

A. Neumaier (1982)

1. Steiner systems 2-$(v, k, 1)$ designs, $x = 0$, $y = 1$.
2. Hadamard 3-design, 2-$(4n, 2n, 2n - 1)$, $x = 0$, $y = n$; more generally, resolvable designs $(x = 0)$
3. residual of biplanes (finitely many known)

Other examples:

1. (if we allow repeated blocks) multiples of symmetric designs.
2. Exceptional designs: not in the above classes.
3. 4-$(23, 7, 1)$ design or its complement is the only quasi-symmetric design which is a 4-design.

Theorem (Harada-M.-Tonchev)

There is no quasi-symmetric 2-$(37, 9, 8)$ design.

Bouyuklieava-Varbanov (2005) showed the non-existence with the assumption that an automorphism of order 5 exists.

Incidence matrix

Suppose that $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a quasi-symmetric 2-$(37, 9, 8)$ design with intersection numbers $x = 1$ and $y = 3$. Let A be its incidence matrix:

$$p \in \mathcal{P}\ (v = 37)$$

$$A = \begin{matrix} B \in \mathcal{B} \\ (b = 148) \end{matrix} \quad \left[A_{B,p} = \begin{cases} 1 & \text{if } p \in B \\ 0 & \text{otherwise} \end{cases} \right]$$

Then

$$A^\top A = 36I + 8(J - I) \quad (r = 36)$$

$$AA^\top = 9I + \begin{bmatrix} 0 & & 1,3 \\ & \ddots & \\ 1,3 & & 0 \end{bmatrix}.$$

Since

$$AA^\top = 9I + \begin{bmatrix} 0 & & 1,3 \\ & \ddots & \\ 1,3 & & 0 \end{bmatrix},$$

we have

$$\begin{bmatrix} A & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix} \begin{bmatrix} A^\top \\ \mathbf{1}^\top \\ \mathbf{1}^\top \\ \mathbf{1}^\top \end{bmatrix} = AA^\top + 3J$$

$$= 12I + \begin{bmatrix} 0 & & 4,6 \\ & \ddots & \\ 4,6 & & 0 \end{bmatrix}$$

$$\equiv 0 \pmod 2.$$

Thus the $\mathbb{F}_2$-linear span of $\begin{bmatrix} A & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix}$ is a doubly even code.

Definition

A code of length m means a $\mathbb{F}_2$-linear subspace of $\mathbb{F}_2^m$. The weight $\mathrm{wt}(\mathbf{u})$ of a vector $\mathbf{u} \in \mathbb{F}_2^m$ is the number of nonzero coordinates of $\mathbf{u}$. A code C is doubly even if

$$\mathrm{wt}(\mathbf{u}) \equiv 0 \pmod 4 \quad (\forall \mathbf{u} \in C).$$

Lemma

If A is a $(0,1)$ matrix such that (diagonals of $AA^\top$) $\equiv 0 \pmod 4$ and $AA^\top \equiv 0 \pmod 2$, then the $\mathbb{F}_2$-linear span of A is a doubly even code.

$$\begin{bmatrix} A & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix} \begin{bmatrix} A^\top \\ \mathbf{1}^\top \\ \mathbf{1}^\top \\ \mathbf{1}^\top \end{bmatrix} = 12I + \begin{bmatrix} 0 & & 4,6 \\ & \ddots & \\ 4,6 & & 0 \end{bmatrix}$$

In our case

$$\text{row space of } \begin{bmatrix} A & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix} \subset \mathbb{F}_2^{40} \text{ is doubly even.}$$

In general, it is difficult to get information of these codes such as dimension, minimum weight.

Definition

For a code C of $\mathbb{F}_2^m$, the minimum weight of C is

$$\min\{\mathrm{wt}(\mathbf{u}) \mid \mathbf{u} \in C,\ \mathbf{u} \neq 0\}.$$

The dual $C^\perp$ is

$$C^\perp = \{\mathbf{u} \in \mathbb{F}_2^m \mid (\mathbf{u}, \mathbf{v}) = 0 \quad (\forall \mathbf{v} \in C)\}.$$

Lemma (Tonchev (1986))

Let A be the incidence matrix of a 2-(v, k, λ) design. Then the duals of the $\mathbb{F}_2$-linear spans of

$$A, \quad \begin{bmatrix} A & \mathbf{1} \end{bmatrix}$$

have minimum weights at least $(r + \lambda)/\lambda$ and $(b + r)/r$, respectively.

Lemma (Harada-M.-Tonchev (2016))

Let A be the incidence matrix of a quasi-symmetric 2-$(37, 9, 8)$ design. If $\mathbf{u}$ is in the dual of the $\mathbb{F}_2$-linear spans of

$$\begin{bmatrix} A & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix},$$

and $\mathbf{u} \notin \{0, (\ldots, 0, 1, 1), (\ldots, 1, 0, 1), (\ldots, 1, 1, 0)\}$, then $\mathrm{wt}(\mathbf{u}) \geq (b + r)/r = (148 + 36)/36 > 5$.

Definition

A doubly even self-dual (d.e.s.d.) $[2n, n]$ code is a doubly even code $C \subset \mathbb{F}_2^{2n}$ with $C = C^{\perp}$. If the minimum weight d, then it is also called a $[2n, n, d]$ code.

- A doubly even self-dual $[2n, n]$ code exists iff $2n \equiv 0 \pmod 8$.
- If $2n \equiv 0 \pmod 8$, then every doubly even code $D \subset \mathbb{F}_2^{2n}$ is contained in some d.e.s.d. $[2n, n]$ code.

Thus

$$\text{row space of } \begin{bmatrix} A & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix} \subset \exists C \text{ a d.e.s.d. } [40, 20, 8] \text{ code,}$$

since

$$\left(\text{row space of } \begin{bmatrix} A & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix}\right)^{\perp}$$

has minimum weight > 5 by the Lemma.

row space of $\begin{bmatrix} A & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix} \subset \exists C$ a d.e.s.d. $[40, 20, 8]$ code.

Theorem (Betsumiya-Harada-M. (2012))

There are 16470 doubly even self-dual $[40, 20, 8]$ codes.

If $\exists$ a quasi-symmetric 2-$(37, 9, 8)$ design, then

$$\exists C\text{: a d.e.s.d. } [40, 20, 8] \text{ code},$$
$$\exists T \subset \{1, \dots, 40\},\ |T| = 3$$

such that $\mathcal{B}$ can be embedded in

$$X = \{\mathrm{supp}(\mathbf{u}) \setminus T \mid \mathbf{u} \in C,\ \mathrm{wt}(\mathbf{u}) = 12,\ \mathrm{supp}(\mathbf{u}) \supset T\}$$
$$\subset \binom{\{1, \dots, 40\} \setminus T}{9}.$$

There are $16470 \times \binom{40}{3}$ ways to choose (C, T).

Search method (1)

There are $16470 \times \binom{40}{3}$ ways to choose (C, T).

$$\mathcal{B} \subset X = \{\mathrm{supp}(\mathbf{u}) \setminus T \mid \mathbf{u} \in C,\ \mathrm{wt}(\mathbf{u}) = 12,\ \mathrm{supp}(\mathbf{u}) \supset T\}.$$

For $\{i, j\} \subset \{1, \ldots, 40\} \setminus T$, let

$$\Gamma_{ij} = \{B \in X \mid B \supset \{i, j\}\}.$$

Then "8-clique"

$$|\mathcal{B} \cap \Gamma_{ij}| = \lambda = 8,$$
$$B, B' \in \mathcal{B} \cap \Gamma_{ij},\ B \neq B' \implies |B \cap B'| = 3.$$

Γ_{ij} must contain such an 8-subset.
This test rules out 15940 of 16470 d.e.s.d $[40, 20, 8]$ codes.

Search method (2)

There are still $16470 - 15940 = 530$ d.e.s.d $[40, 20, 8]$ codes which passes the previous test.

Fix $\{i_0, j_0\} \subset \{1, \ldots, 40\} \setminus T$ and enumerate

$$\mathcal{K} = \{\text{8-cliques in } \Gamma_{i_0,j_0}\}.$$

Then $\forall K \in \mathcal{K}$, and $\forall \{i, j\} \subset \{1, \ldots, 40\} \setminus T$ the set

$$\Gamma'_{ij} = \{B' \in \Gamma_{ij} \mid |B \cap B'| \in \{1, 3, 9\} \ (\forall B \in K)\}$$

must have a 8-clique.

We have verified that this is not the case for the remaining 530 codes.

Theorem (Harada-M.-Tonchev)

There is no quasi-symmetric 2-$(37, 9, 8)$ design.

Further problems:

1. ?$\exists$ a strongly regular graph with parameters $(v, k, \lambda, \mu) = (148, 84, 50, 44)$ (could have been obtained if there were a quasi-symmetric 2-$(37, 9, 8)$ design)
2. ?$\exists$ a symmetric 2-$(149, 37, 9)$ design (its derived design is 2-$(37, 9, 8)$ design which can't be quasi-symmetric)
3. ?$\exists$ a quasi-symmetric 2-$(112, 28, 9)$ design with intersection number $x = 6$, $y = 8$ $(112 = 149 - 37)$
4. ?$\exists$ a 1-$(36, 8, 8)$ design with intersection numbers $0, 2$
5. ?$\exists$ a quasi-symmetric 2-$(41, 9, 9)$ design with intersection number $x = 1$, $y = 3$

Thank you for your attention!