Non-existence of block-transitive subspace designs

Dan Hawtin[a]

September 1, 2022 – Irsee, Finite Geometries

University of Rijeka, Croatia
(joint work with Jesse Lansdown)

[a]Supported by the Croatian Science Foundation under the project 6732.

Block designs

Definition

A t-(n, k, λ) design is a pair $\mathscr{D} = (\mathscr{P}, \mathscr{B})$ where:

- Elements of the n-set $\mathscr{P}$ are called *points*.
- Elements of $\mathscr{B}$ are k-subsets of $\mathscr{P}$ called *blocks*.
- **Each t-subset of $\mathscr{P}$ is contained in precisely λ blocks.**

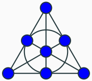
Block designs

Definition

A t-(n, k, λ) design is a pair $\mathscr{D} = (\mathscr{P}, \mathscr{B})$ where:

- Elements of the n-set $\mathscr{P}$ are called *points*.
- Elements of $\mathscr{B}$ are k-subsets of $\mathscr{P}$ called *blocks*.
- **Each t-subset of $\mathscr{P}$ is contained in precisely λ blocks.**

Examples:



- A projective plane of order s is a 2-$(s^2 + s + 1, s + 1, 1)$ design.
- An affine plane of order s is a 2-$(s^2, s, 1)$ design.
- Ex. with $\lambda > 1$ are provided by subspaces/flats of dim. ≥ 2 in other finite geometries.
- Witt designs (rel. to Mathieu groups) give examples with $t \geq 3$.

Symmetry and designs

A fair amount of study has been devoted to the following classes of designs:

- 2-Transitive designs.
- Flag-transitive designs.
- Block-transitive designs.

The examples arising in each case are simply too numerous for a classification to be feasible.

q-Analogues

A q-*analogue* involves introducing a parameter q in such a way that the limit $q \longrightarrow 1$ gives back the classical version.

q-Analogues

A q-*analogue* involves introducing a parameter q in such a way that the limit $q \longrightarrow 1$ gives back the classical version.

For instance, the q-analogue of an integer is:

$$(n)_q = \frac{q^n - 1}{q - 1} = q^{n-1} + q^{n-2} + \cdots + q + 1.$$

And the q-analogue of the binomial coefficient is:

$$\binom{n}{k}_q = \frac{(n)_q(n-1)_q \cdots (n-k+1)_q}{(k)_q(k-1)_q \cdots (1)_q}.$$

Notice that $\binom{n}{k}_q$ counts the number of k-subspaces of $\mathbb{F}_q^n$.

q-Analogues

A q-*analogue* involves introducing a parameter q in such a way that the limit $q \longrightarrow 1$ gives back the classical version.

For instance, the q-analogue of an integer is:

$$(n)_q = \frac{q^n - 1}{q - 1} = q^{n-1} + q^{n-2} + \cdots + q + 1.$$

And the q-analogue of the binomial coefficient is:

$$\binom{n}{k}_q = \frac{(n)_q (n-1)_q \cdots (n-k+1)_q}{(k)_q (k-1)_q \cdots (1)_q}.$$

Notice that $\binom{n}{k}_q$ counts the number of k-subspaces of $\mathbb{F}_q^n$.

Tits (1957) suggested that the combinatorics of $\mathbb{F}_q$-vector spaces as a q-analogue of combinatorics of sets.

Subspace designs

Definition

A t-$(n, k, \lambda)_q$ design is a pair $\mathscr{D} = (V, \mathscr{B})$ where:

- $V \cong \mathbb{F}_q^n$
- Elements of $\mathscr{B}$ are k-subspaces of V called *blocks*.
- **Each t-subspace of V is contained in precisely λ blocks.**

Subspace designs

Definition

A t-$(n, k, \lambda)_q$ design is a pair $\mathscr{D} = (V, \mathscr{B})$ where:

- $V \cong \mathbb{F}_q^n$
- Elements of $\mathscr{B}$ are k-subspaces of V called *blocks*.
- **Each t-subspace of V is contained in precisely λ blocks.**

Example

Regular spread via field reduction:

- Let $V = \mathbb{F}_q^n$ and $U = \mathbb{F}_{q^k}^t$, where $n = kt$.
- As $\mathbb{F}_q$-vector spaces $V \cong U$.
- The set of 1-dim. $\mathbb{F}_{q^k}$-subspaces of U corresponds a set $\mathscr{B}$ of k-dim. $\mathbb{F}_q$-subspaces of V.
- $(V, \mathscr{B})$ is a 1-$(n, k, 1)_q$ design.

Examples of subspace designs

The following designs have been constructed with $t \geq 2$[1]:

- $2\text{-}(n, 3, 7)_2$ designs when $\gcd(n, 6) = 1$, Thomas (1987).
- $2\text{-}(n, q + 1, q^2 + q + 1)_q$ designs when $\gcd(n, 6) = 1$, Suzuki (1990,1992).
- Braun, Kerber and Laue (2005) found various 2-designs via computer search, as well as $3\text{-}(8, 4, \lambda)_2$ designs for $\lambda = 11$ and $\lambda = 20$.
- $2\text{-}(13, 3, 1)_2$ designs, the first examples of q-*Steiner systems*[2], Braun et al. (2016).

Automorphism groups are normalisers of Singer cycles.

[1] Note that we are only interested in $t \geq 2$ in what follows.

[2] A subspace design with $\lambda = 1$.

Divisors and duality

Lemma

If $t \geq 2$ and $\mathscr{D} = (V, \mathscr{B})$ is a t-$(n, k, \lambda)_q$ design then $\mathscr{D}$ is also a 2-$(n, k, \lambda_2)_q$ design, for some integer λ_2. In particular,

$$|\mathscr{B}| = \frac{(n)_q(n-1)_q}{(k)_q(k-1)_q}\lambda_2.$$

Lemma

Let $\mathscr{D} = (\mathscr{P}, \mathscr{B})$ be a t-$(n, k, \lambda)_q$ design and let $\mathscr{B}^\perp = \{U^\perp \mid U \in \mathscr{B}\}$, where $\perp$ is a duality on V.

Then $\mathscr{D}^\perp = (\mathscr{P}, \mathscr{B}^\perp)$ is a t-$(n, n-k, \lambda')_q$ design, for some integer λ'.

Divisors and duality

Lemma

If $t \geq 2$ and $\mathscr{D} = (V, \mathscr{B})$ is a t-$(n, k, \lambda)_q$ design then $\mathscr{D}$ is also a 2-$(n, k, \lambda_2)_q$ design, for some integer λ_2. In particular,

$$|\mathscr{B}| = \frac{(n)_q(n-1)_q}{(k)_q(k-1)_q}\lambda_2.$$

Lemma

Let $\mathscr{D} = (\mathscr{P}, \mathscr{B})$ be a t-$(n, k, \lambda)_q$ design and let $\mathscr{B}^\perp = \{U^\perp \mid U \in \mathscr{B}\}$, where $\perp$ is a duality on V.

Then $\mathscr{D}^\perp = (\mathscr{P}, \mathscr{B}^\perp)$ is a t-$(n, n-k, \lambda')_q$ design, for some integer λ'.

We can focus on 2-$(n, k, \lambda)_q$ designs with $k \leq n/2$.

Automorphism groups

The *Grassmann graph* $J_q(n, k)$ is the graph with vertex set all k-subspaces of $\mathbb{F}_q^n$; two vertices are adjacent when they intersect in a $(k-1)$-subspace.

Lemma

For $2 \leq k \leq n-2$, the automorphism group of $J_q(n, k)$ is:

- $P\Gamma L_n(q)$ when $n \neq 2k$.
- $P\Gamma L_n(q).C_2$ when $n = 2k$.

(In the second case the map $U \mapsto U^{\perp}$ is an automorphism.)

Automorphism groups

The *Grassmann graph* $J_q(n, k)$ is the graph with vertex set all k-subspaces of $\mathbb{F}_q^n$; two vertices are adjacent when they intersect in a $(k-1)$-subspace.

Lemma

For $2 \leq k \leq n-2$, the automorphism group of $J_q(n, k)$ is:

- $P\Gamma L_n(q)$ when $n \neq 2k$.
- $P\Gamma L_n(q).C_2$ when $n = 2k$.

(In the second case the map $U \mapsto U^{\perp}$ is an automorphism.)

A subspace design $\mathscr{D}$ may be thought of as a code in a Grassmann graph, and $\mathrm{Aut}(\mathscr{D})$ is then the setwise stabiliser of $\mathscr{B}$ in $P\Gamma L_n(q)$ (unless $\mathscr{D}$ is self-dual).

Block transitivity

Definition

We say that a t-$(n, k, \lambda)_q$ design $\mathcal{D} = (V, \mathcal{B})$ is *block-transitive* if $\mathrm{Aut}(\mathcal{D})$ acts transitively on $\mathcal{B}$.

Block transitivity

Definition

We say that a t-$(n, k, \lambda)_q$ design $\mathscr{D} = (V, \mathscr{B})$ is *block-transitive* if $\mathrm{Aut}(\mathscr{D})$ acts transitively on $\mathscr{B}$.

Recall that we can focus on the case $t = 2$ and $k \leq n/2$.

Lemma

Suppose $\mathscr{D} = (V, \mathscr{B})$ is a block-transitive 2-$(n, k, \lambda)_q$ design. Then $\mathrm{Aut}(\mathscr{D})$ is a subgroup of $P\Gamma L_n(q)$ and has order divisible by

$$|\mathscr{B}| = \frac{(n)_q(n-1)_q}{(k)_q(k-1)_q}\lambda.$$

Primitive divisors and Zsigmondy's Theorem

Definition

A divisor r of $q^m - 1$ that is coprime to $q^i - 1$ for all $i < m$ is called a *primitive divisor* of $q^m - 1$.

- If r is prime then r is called a *primitive prime divisor*.
- The largest primitive divisor is called the *primitive part*.
- Note that r divides $(m)_q$ and is coprime to $(i)_q$ for all $i < m$.

[3] Note that the theorem is actually a fair bit more general than this.

Primitive divisors and Zsigmondy's Theorem

Definition

A divisor r of $q^m - 1$ that is coprime to $q^i - 1$ for all $i < m$ is called a *primitive divisor* of $q^m - 1$.

- If r is prime then r is called a *primitive prime divisor*.
- The largest primitive divisor is called the *primitive part*.
- Note that r divides $(m)_q$ and is coprime to $(i)_q$ for all $i < m$.

Theorem (Zsigmondy's Theorem)[3]

Primitive prime divisors exist except for when $q^m = 2^6$.

[3] Note that the theorem is actually a fair bit more general than this.

Applications of Zsigmondy's Theorem

Hering's Theorem (1985):

- Classified transitive linear groups.

Guralnick, Pentilla, Praeger, Saxl (1999):

- Classified groups $G \leq GL_n(q)$ such that $|G|$ is divisible by some primitive prime divisor of $q^e - 1$, where $n/2 < e \leq n$.

Bamberg and Pentilla (2008):

- Classified groups $G \leq GL_n(q)$ such that $|G|$ is divisible by the primitive part r of $q^e - 1$, where $r > 1$ and $n/2 < e \leq n$.

Applying Bamberg and Pentilla

Recall that if $\mathscr{D} = (V, \mathscr{B})$ is a block-transitive t-$(n, k, \lambda)_q$ design then $|\mathrm{Aut}(\mathscr{D})|$ is divisible by

$$|\mathscr{B}| = \frac{(n)_q(n-1)_q}{(k)_q(k-1)_q}\lambda_2.$$

In particular, $|\mathrm{Aut}(\mathscr{D})|$ is divisible by each of the primitive parts r_n and r_{n-1} of $q^n - 1$ and $q^{n-1} - 1$, respectively.

Applying Bamberg and Pentilla

Recall that if $\mathscr{D} = (V, \mathscr{B})$ is a block-transitive t-$(n, k, \lambda)_q$ design then $|\operatorname{Aut}(\mathscr{D})|$ is divisible by

$$|\mathscr{B}| = \frac{(n)_q(n-1)_q}{(k)_q(k-1)_q}\lambda_2.$$

In particular, $|\operatorname{Aut}(\mathscr{D})|$ is divisible by each of the primitive parts r_n and r_{n-1} of $q^n - 1$ and $q^{n-1} - 1$, respectively.

By the result of Bamberg and Pentilla, we than have the following cases:

1. One of r_n, r_{n-1} is equal to 1.
2. $r_n, r_{n-1} \neq 1$, r_n, r_{n-1} divide $|G|$ and $G \leq \Gamma L_1(q^n)$.
3. $r_n, r_{n-1} \neq 1$ and r_n, r_{n-1} divide $|G \cap GL_n(q)|$.

Applying Bamberg and Pentilla

Cases:

1. One of r_n, r_{n-1} is equal to 1.
2. $r_n, r_{n-1} \neq 1$, r_n, r_{n-1} divide $|G|$ and $G \leq \Gamma L_1(q^n)$.
3. $r_n, r_{n-1} \neq 1$ and r_n, r_{n-1} divide $|G \cap GL_n(q)|$.

Eliminate via:

1. Subgroup structure and geometric arguments.
2. Divisibility conditions and geometric arguments leave one case, a hypothetical 2-$(11, 5, 5)_2$ design. Ruled out via a lengthy computation.
3. Apply Bamberg and Pentilla - divisibility conditions eliminate any remaining cases.

Main theorem

Theorem (H., Lansdown)

There are no non-trivial block-transitive t-$(n, k, \lambda)_q$ designs for $t \geq 2$.

Main theorem

Theorem (H., Lansdown)

There are no non-trivial block-transitive t-$(n, k, \lambda)_q$ designs for $t \geq 2$.

A subspace design with $\lambda = 1$ is called a q-Steiner system.

Corollary (H., Lansdown)

There are no block-transitive q-Steiner systems.

Thanks for listening!

RICOTTA2023 at the University of Rijeka, Croatia.

July 3–7, 2023.

https://riccota2023.math.uniri.hr/

Rijeka Conference on Combinatorial Objects and their Applications