Large sets of infinite-dimensional q-Steiner systems

Dan Hawtin

45ACC UWA

Faculty of Mathematics, University of Rijeka

Infinite designs

[P.J. Cameron, B.S. Webb. What is an infinite design? *Journal of Combinatorial Designs*, 10(2):79–91, 2002.]

- Discusses designs on infinite sets.
- Underlying set may be countably or uncountably infinite.
- Block size may be finite or infinite.
- Gives several families of examples and some existence results.

Steiner systems

Definition (Steiner system)

If $\mathscr{V}$ is a set, then an $S(t, k, \mathscr{V})$ is a collection $\mathscr{B}$ of k-subsets of $\mathscr{V}$ such that every t-subset of $\mathscr{V}$ is contained in precisely one element of $\mathscr{B}$.

Some finite examples:

- A projective plane of order k is an $S(2, k+1, [k^2+k+1])$.
- An affine plane of order k is an $S(2, k, [k^2])$.
- The Witt designs are Steiner systems with $t = 3, 4$ or 5.

There are no known (finite) $S(t, k, \mathscr{V})$ for $t \geq 6$.
However, by a result of Keevash (2014), they must exist.

Large sets

Definition (Large set)

An $LS(t, k, \mathscr{V})$ is a collection of $S(t, k, \mathscr{V})$ systems that form a partition of the set of all k-subsets of $\mathscr{V}$.

Examples:

- Lu (and subsequently Teirlinck) constructed an $LS(2, 3, \mathscr{V})$ with $7 \neq |\mathscr{V}| \equiv 1, 3 \pmod 6$ (all possible values).
- An $LS(2, 4, \mathscr{V})$ exists with $|\mathscr{V}| = 13$ (Chouinard 1983) and $|\mathscr{V}| = 16$ (Mathon 1997).
- Grannell *et al.* (1991) gave an explicit construction for $LS(t, t + 1, \mathscr{V})$ systems, $\mathscr{V}$ countably and uncountably infinite.

q-Steiner systems

Definition (q-Steiner system)

If V is a vector-space over $\mathbb{F}_q$, then an $S(t, k, V)_q$, is a collection $\mathscr{B}$ of k-spaces of V such that every t-space of V is contained in precisely one element of $\mathscr{B}$.

- If $t = 1$ then this is a spread.
- For $t \geq 2$, only known examples are $S(2, 3, V)_2$ systems, where $\dim V = 13$ (Braun *et al.* 2016).
- Asymptotic existence (Ray-Chaudhuri and Singhi, 1989).
- No known infinite-dimensional examples.

Existence

Definition (Large set)

An $LS(t,k,V)_q$ is a collection of $S(t,k,V)_q$ systems that form a partition of the set of all k-subspaces of V.

Theorem (Cameron 1995)

(Roughly) Large sets of $LS(t,k,\mathscr{V})$ and $LS(t,k,V)_q$ exist for all $1 < t < k$ when $|\mathscr{V}|$ or $\dim V$ has any infinite cardinality.

Linearised polynomials

Let F be the algebraic closure of $\mathbb{F}_q$.

Definition

A *linearised polynomial* or q*-polynomial* is a polynomial $f \in F[x]$ of the form

$$f = a_0 x + a_1 x^q + \cdots + a_k x^{q^k}.$$

Linearised polynomials

Let F be the algebraic closure of $\mathbb{F}_q$.

Definition

A *linearised polynomial* or *q-polynomial* is a polynomial $f \in F[x]$ of the form

$$f = a_0 x + a_1 x^q + \cdots + a_k x^{q^k}.$$

If $a, b \in F$ then $(a+b)^{q^i} = a^{q^i} + b^{q^i}$.

- $f : F \longrightarrow F; x \mapsto f(x)$ is $\mathbb{F}_q$-linear.
- The roots of f form an $\mathbb{F}_q$-linear subspace of F.

If $a_k \neq 0$ then we say f has *q-degree* k.

Linearised polynomials

A few applications of linearised polynomials:

- permutation polynomials
- rank-distance codes
- linear sets

Linearised polynomials

A few applications of linearised polynomials:

- permutation polynomials
- rank-distance codes
- linear sets

Question

Is there a natural way to construct a q-Steiner system from a family of linearised polynomials?

Coefficients and determinants

Let $V = \langle v_1, \ldots, v_k \rangle$ be a k-dimensional $\mathbb{F}_q$-subspace of F and let

$$f = \begin{vmatrix} x & x^q & x^{q^2} & \cdots & x^{q^k} \\ v_1 & v_1^q & v_1^{q^2} & \cdots & v_1^{q^k} \\ v_2 & v_2^q & v_2^{q^2} & \cdots & v_2^{q^k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_k & v_k^q & v_k^{q^2} & \cdots & v_k^{q^k} \end{vmatrix}.$$

Then f is a q-degree k linearised polynomial with roots V.

Coefficients and determinants

Let $V = \langle v_1, \ldots, v_k \rangle$ be a k-dimensional $\mathbb{F}_q$-subspace of F and let

$$f = \begin{vmatrix} x & x^q & x^{q^2} & \cdots & x^{q^k} \\ v_1 & v_1^q & v_1^{q^2} & \cdots & v_1^{q^k} \\ v_2 & v_2^q & v_2^{q^2} & \cdots & v_2^{q^k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_k & v_k^q & v_k^{q^2} & \cdots & v_k^{q^k} \end{vmatrix}.$$

Then f is a q-degree k linearised polynomial with roots V.

The coefficient of x^{q^i} in f is the determinant of the $(k \times k)$-minor obtained by deleting the top row and the column containing x^{q^i}.

The construction

For $a \in F^\times$ and $B = (b_1, \dots, b_t) \in F^t$, define

$$f_{a,B} = a^q x + b_1 x^q + \cdots + b_t x^{q^t} + a x^{q^{t+1}}.$$

Furthermore, define

$$\mathscr{B}_a = \{\ker f_{a,B} \mid B \in F^t\}.$$

Theorem (DRH 2023+)

The set $\{\mathscr{B}_a \mid a \in F^\times\}$ is an $LS(t, t+1, F)_q$ for any $t \geq 1$ and any prime power q.

One part of the proof

Let $B, C \in F^t$. Then

$$\begin{aligned} f_{a,B} - f_{a,C} &= (b_1 - c_1)x^q + \cdots + (b_t - c_t)x^{q^t} \\ &= g^q, \end{aligned}$$

for some linearised polynomial g with q-degree $t-1$.

- The GCD of $f_{a,B}$ and $f_{a,C}$ divides g.
- $\ker g$ has dimension at most $t-1$.

Thus, any pair of distinct elements of $\mathscr{B}_a$ intersect in at most a $(t-1)$-space.

What next?

Question

Can a similar construction produce an $LS(t,k,F)_q$ for all t,k with $0 < t < k$?

Thanks for listening!

Enjoy the excursion!