Lifting of Divisible Designs

Joint work with
Andrea Blunck (Hamburg) and Corrado Zanella (Vicenza)

TU WIEN
Technische Universität Wien
Vienna University of Technology
Differentialgeometrie und Geometrische Strukturen

Hans Havlicek
Forschungsgruppe Differentialgeometrie und Geometrische Strukturen
Institut für Diskrete Mathematik und Geometrie
Technische Universität Wien
havlicek@geometrie.tuwien.ac.at

Divisible Designs

Assume that X is a finite set of *points*, endowed with an equivalence relation $\mathcal{R}$; its equivalence classes are called *point classes*. A subset Y of X is called *$\mathcal{R}$-transversal* if for each point class C we have

$$\#(C \cap Y) \leq 1.$$

Let us recall the following:

Definition. A triple $\mathcal{D} = (X, \mathcal{B}, \mathcal{R})$ is called a *t-(s, k, λ_t)-divisible design* (DD) if there exist positive integers t, s, k, λ_t such that the following axioms hold:

(A) $\mathcal{B}$ is a set of $\mathcal{R}$-transversal subsets of X, called *blocks*, with $\#B = k$ for all $B \in \mathcal{B}$.

(B) Each point class has size s.

(C) For each $\mathcal{R}$-transversal t-subset $Y \subset X$ there exist exactly λ_t blocks containing Y.

(D) $t \leq \frac{v}{s}$, where $v := \#X$.

Constructions of t-DDs

- Construction of A. G. Spera (1992):

  Uses a finite set X endowed with an equivalence relation on X, a base block $B \subset X$, and a group G acting on X such that ...

  C. Cerroni, S. Giese, R. H. Schulz, and A. G. Spera obtained 2-DDs and 3-DDs in this way.

  Cf. D. R. Hughes (1965).

- Construction of S. Giese (2005) for $t = 2$:

  Uses the dual space of $\mathrm{PG}(n+1, q)$, a hyperplane H of $\mathrm{PG}(n+1, q)$, an origin (a point off H), a starter 2-DD embedded in the dual space such that ..., and the group of translations with respect to H.

t-Lifting

Theorem 1. Let X be a finite set, let t be a fixed positive integer, let $(\overline{X}, \overline{\mathcal{B}}, \overline{\mathcal{R}})$, where $\overline{X} \subset X$, be a t-$(\overline{s}, k, \overline{\lambda}_t)$-divisible design, and let G be a group acting on X. Suppose, furthermore, that the following properties hold:

1. For each $x \in X$ there is a unique element of $\overline{X}$, say $\widehat{x}$, such that $x^G = \widehat{x}^G$.

...

5. All setwise stabilizers $G_{\overline{B}}$, where $\overline{B} \in \overline{\mathcal{B}}$ is any block, have the same cardinality.

Define

$$\mathcal{B} := \overline{\mathcal{B}}^G = \{\overline{B}^g \mid \overline{B} \in \overline{\mathcal{B}}, g \in G\} \text{ and } \mathcal{R} := \{(x, x') \in X \times X \mid (\widehat{x}, \widehat{x}') \in \overline{\mathcal{R}}\}.$$

Then $(X, \mathcal{B}, \mathcal{R})$ is a t-(s, k, λ_t)-divisible design, where

$$s = (\#\overline{x}^G)\overline{s}, \quad \lambda_t := \overline{\lambda}_t \frac{\#G_{\overline{Y}}}{\#G_{\overline{B}}}$$

with arbitrary $\overline{x}$, $\overline{Y}$, and $\overline{B}$ as above.

Geometric examples

Theorem 2. Let t be a fixed positive integer and let $(\overline{X}, \overline{\mathcal{B}}, \overline{\mathcal{R}})$ be a t-$(\overline{s}, k, \overline{\lambda}_t)$ divisible design with the following properties:

1. $\overline{X}$ is a set of $\overline{v}$ points generating a finite projective space $\mathrm{PG}(d, q)$.
2. All $\overline{\mathcal{R}}$-transversal t-subsets of $\overline{X}$ are independent in $\mathrm{PG}(d, q)$.
3. All blocks in $\overline{\mathcal{B}}$ generate subspaces of $\mathrm{PG}(d, q)$ with the same dimension $\beta - 1$.

Then for each non-negative integer c there exists a t-$(q^c\overline{s}, k, q^{c(\beta-t)}\overline{\lambda}_t)$-divisible design with $q^c\overline{v}$ points.

Proof. Let $n := d + c$. Consider in $\mathrm{PG}(n, q)$ the cone with base $\overline{X}$, whose vertex is a $\mathrm{PG}(c - 1, q)$ skew to $\mathrm{PG}(d, q)$, and the group G of all matrices

$$\begin{pmatrix} I_{d+1} & M \\ 0 & I_c \end{pmatrix} \in \mathrm{GL}_{n+1}(q).$$

Put $X :=$ cone $\setminus$ vertex. Now Theorem 1 can be applied. $\square$

Small Witt design

The *small Witt design* W_{12} is a 5-$(1, 6, 1)$-DD (i.e. a design) with 12 points. By a result of H. S. M. Coxeter (1958), W_{12} can be embedded in $\mathrm{PG}(5, 3)$ in such a way that the following properties hold:

(i) The point set $\overline{X}$ of W_{12} generates $\mathrm{PG}(5, 3)$.

(ii) All 5-subsets of $\overline{X}$ are independent.

(iii) All blocks span hyperplanes of $\mathrm{PG}(5, 3)$.

We can apply Theorem 2 to construct 5-$(3^c, 6, 1)$-DDs from W_{12} and (disregarding the blocks of W_{12}) transversal 5-$(3^c, 12, 3^c)$-DDs, each with with $12 \cdot 3^c$ points.

Large Witt design

The *large Witt design* W_{24} is a 5-$(1, 8, 1)$-DD (i.e. a design) with 24 points. By a result of J. A. Todd (1959), W_{24} can be embedded in $\mathrm{PG}(11, 2)$ in such a way that the following properties hold:

(i) The point set $\overline{X}$ of W_{24} generates $\mathrm{PG}(11, 2)$.

(ii) All 5-subsets of $\overline{X}$ are independent.

(iii) All blocks span 6-dimensional subspaces of $\mathrm{PG}(11, 2)$.

We can apply Theorem 2 to construct 5-$(2^c, 8, 1)$-DDs from W_{24} and (disregarding the blocks of W_{24}) transversal 5-$(2^c, 24, 3^{7c})$-DDs, each with $24 \cdot 2^c$ points.

Veronese varieties

A Veronese variety $\mathcal{V}_{m,t-1}$ is the image of $\mathrm{PG}(m,q)$ under the Veronese mapping

$$\mathrm{PG}(m,q) \to \mathrm{PG}(d,q) \text{ with } d = \binom{m+t-1}{m} - 1,\ t \geq 2.$$

The Veronesean $\mathcal{V}_{m,t-1}$ has $k := q^m + q^{m-1} + \cdots + 1$ points and can be considered as a t-design with just one block. The following properties hold:

(i) The Veronesean $\mathcal{V}_{m,t-1}$ generates $\mathrm{PG}(d,q)$ if, and only if, $t \leq q+1$ (G. Tallini, 1961).

(ii) All t-subsets of $\overline{X}$ are independent.

For any $t \geq 2$ there is a prime power q such that $t \leq q+1$.

So, we can apply Theorem 2 to construct transversal t-$(q^c, k, q^{c(d-t+1)})$-DDs.

Final remarks

- Also other point sets like elliptic quadrics, caps, . . . can be used to construct transversal DDs.

- In affine terms, the DDs arising from Veroneseans are closely related with the interpolation formula of Lagrange.

A. Blunck, H. Havlicek, and C. Zanella: Lifting of divisible designs. *Designs, Codes and Cryptography* (to appear).