Designs in affine geometry

Jens Zumbrägel
Computer and Communication Sciences
EPFL, Lausanne

Network Coding and Designs
Dubrovnik · April 4 - 8, 2016

```
2012
BrusselsAscona
BarcelonaBerge
nZurichGhentTa
llinBordeauxPa
lmelaBanzNoviS
adSalamancaIst
anbulDubrovnik
          2016
```

Introduction

- Classical designs and their (projective) q-analogs can both be viewed as *designs in matroids*.
- Not much known on q-analogs of designs.
  - construction of such designs by Thomas (1987) and others
  - Steiner system $S(2,3,13)$ has been found (2012)
  - existence of Fano plane $S(2,3,7)$ still unknown
- Another natural matroid is given by the point sets in general position of an affine space.
- What is the relationship between the affine and the projective q-analogs of designs?
- Do there exist affine Steiner systems?

Outline

1. A short recap of matroid theory
2. Matroid examples from finite geometry
3. Affine and projective designs
4. Observations and questions

Matroids – an abstraction of linear independence

Definition

A matroid is a pair $(S, \mathcal{I})$, where S is a finite set and $\mathcal{I}$ is a nonempty family of *independent* subsets of S satisfying

(i) if $I \in \mathcal{I}$ and $J \subseteq I$, then $J \in \mathcal{I}$;

(ii) (*exchange axiom*) if $I, J \in \mathcal{I}$ and $|I| < |J|$, then there is $x \in J \setminus I$ with $I \cup \{x\} \in \mathcal{I}$.

Examples

1. The *free matroid* $(S, \mathcal{P}(S))$, where S is a finite set.
2. The *vector matroid* $(V, \mathcal{I})$, where $\mathcal{I}$ is the family of all linearly independent subsets of a finite vector space V.
3. The *graphic matroid* $(E, \mathcal{I})$, where $G = (V, E)$ is a graph, $E \subseteq \binom{V}{2}$, and a subset of E is independent iff it contains no cycle.

For any matroid $M = (S, \mathcal{I})$ and any subset X of S the *restriction* $M|X := (X, \mathcal{I} \cap \mathcal{P}(X))$ is again a matroid.

Rank and basis

Let $M = (S, \mathcal{I})$ be a matroid.

Definition

The rank $\rho(X)$ of a subset X of S is the cardinality of a maximal independent subset of X. By the exchange axiom this is well-defined.

The closure operator $\mathrm{cl} : \mathcal{P}(S) \to \mathcal{P}(S)$ is defined by

$$\mathrm{cl}(X) := \{x \in S \mid \rho(X \cup \{x\}) = \rho(X)\}.$$

A subset X of S satisfying $X = \mathrm{cl}(X)$ is called a *flat*, or a k-*flat* if its rank is k. For each flat X and all $x, y \in S \setminus X$ there holds the *exchange property:* $y \in \mathrm{cl}(X \cup \{x\}) \;\Rightarrow\; x \in \mathrm{cl}(X \cup \{y\})$.

A subset X of S is called *generating* if $\mathrm{cl}(X) = S$.
maximal independent = independent generating = minimal generating
Such a set is called basis.

Designs in matroids

A *perfect matroid design* (PMD) is a matroid M of some rank n for which any k-flat has the same cardinality f_k, where $0 \leq k \leq n$.

Examples

1. The free matroid $(S, \mathcal{P}(S))$, where $|S| = n$.
2. The vector matroid $(V, \mathcal{I})$, where $\dim V = n$.

Geometrization: Let M be a PMD. By deleting elements $x \in S$ such that $\{x\} \notin \mathcal{I}$ and identifying elements $x, y \in S$ such that $\{x, y\} \notin \mathcal{I}$, we get again a PMD M'.
Example: vector space $\rightsquigarrow$ projective space.

Definition

A t-(n, k, λ) design *in* M is a collection $\mathcal{B}$ of k-flats in M such that each t-flat in M is contained in exactly λ members of $\mathcal{B}$.

Any t-(n, k, λ) design in M is also an s-(n, k, λ_s) design for $s < t$.

Outline

1 A short recap of matroid theory

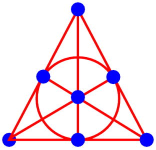
2 Matroid examples from finite geometry

3 Affine and projective designs

4 Observations and questions

PMDs from incidence geometry

Let $\mathbf{G} = (\mathcal{P}, \mathcal{L}, I)$ be an *incidence space*, with point set $\mathcal{P}$, line set $\mathcal{L}$ and incidence relation $I \subseteq \mathcal{P} \times \mathcal{L}$. A set $\mathcal{U}$ of points is called a *linear set* if $(PQ) \subseteq \mathcal{U}$ for any two points P, Q of $\mathcal{U}$. The *span* $\mathrm{cl}(\mathcal{X})$ of a subset $\mathcal{X}$ of $\mathcal{P}$ is the smallest linear set containing $\mathcal{X}$. A set of points $\mathcal{B}$ is *independent* if $P \notin \mathrm{cl}(\mathcal{B} \setminus \{P\})$ for all $P \in \mathcal{B}$.



Let $\mathbf{G}$ be a *projective space* or an *affine space*. Then:

- For any linear set $\mathcal{U}$ and points $P, Q \notin \mathcal{U}$ the *exchange property* $Q \in \mathrm{cl}(\mathcal{U} \cup \{P\}) \;\Rightarrow\; P \in \mathrm{cl}(\mathcal{U} \cup \{Q\})$ holds.
- Then $M_{\mathbf{G}} := (\mathcal{P}, \mathcal{I})$ is a matroid, where $\mathcal{I} = \{\,\text{independent sets}\,\}$.
- One defines $\dim \mathbf{G} = |\mathcal{B}| - 1$, where $\mathcal{B}$ is a basis. Thus: geometric dimension $=$ matroid rank $- 1$.
- All t-dimensional subspaces have the same number of points, i.e., the matroid of independent sets is a perfect matroid design.

Designs in finite geometries

Let $\mathbf{G} = (\mathcal{P}, \mathcal{L}, I)$ be a projective or an affine space of dimension $v-1$.

Definition

A t-(v, k, λ) design *in* $\mathbf{G}$ is a collection $\mathcal{B}$ of $(k-1)$-dimensional subspaces of $\mathbf{G}$, called *blocks*, such that every $(t-1)$-dimensional subspace of $\mathbf{G}$ is contained in exactly λ blocks.

If $\mathbf{G} = \mathbf{P}$ is a projective space we refer to a t-(v, k, λ) *projective* design, and in case $\mathbf{G} = \mathbf{A}$ is an affine space to an t-(v, k, λ) *affine* design.

If $\lambda = 1$ we speak of a (projective or affine) Steiner system $S(t, k, v)$.

Let $\mathbf{P} = \mathbf{P}(V)$ be the projective space associated to a vector space V. Then a t-(v, k, λ) projective design in $\mathbf{P}$ corresponds to a t-(v, k, λ) subspace design in V, i.e., a collection $\mathcal{B}$ of k-dim. subspaces of V such that each t-dim. subspace of V is contained in exactly λ members of $\mathcal{B}$.

Outline

1 A short recap of matroid theory

2 Matroid examples from finite geometry

3 Affine and projective designs

4 Observations and questions

Affine designs from projective designs

Let V be a vector space and let T be its group of translations.

Theorem

Suppose that $\mathcal{B}$ is a t-(v,k,λ) subspace design in V, then $T\mathcal{B} := \{\alpha U \mid U \in \mathcal{B}, \alpha \in T\}$ is an $(t+1)$-$(v+1,k+1,\lambda)$ affine design.

Conversely, if $\mathcal{D}$ is an $(t+1)$-$(v+1,k+1,\lambda)$ affine design in $\mathbf{A}(V)$, then $\mathcal{D}_0 := \{W \in \mathcal{D} \mid 0 \in W\}$ is a t-(v,k,λ) subspace design.

$$t\text{-}(v,k,\lambda) \qquad \longleftrightarrow \qquad (t+1)\text{-}(v+1,k+1,\lambda)$$

projective designs ⟷ *affine* designs

Relations with classical designs

Proposition

For any 2-(v, k, λ) projective design of order q there is a 2-$([v]_q, [k]_q, \lambda)$ classical design, $[d]_q := \frac{q^d-1}{q-1}$.

For any 2-(v, k, λ) affine design of order q there is a 2-$(q^{v-1}, q^{k-1}, \lambda)$ classical design; for any 3-(v, k, λ) affine design of order $q = 2$ there is a 3-$(2^{v-1}, 2^{k-1}, \lambda)$ classical design.

Corollary (cf. [EV11, Th. 4])

For any 2-(v, k, λ) *projective design of order* 2 *there is a* 3-$(2^v, 2^k, \lambda)$ *classical design. In particular, for any* $S(2, 3, v)$ *projective Steiner system we obtain a classical* $S(3, 8, 2^v)$ *Steiner system.*

Outline

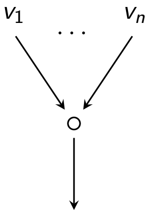
1. A short recap of matroid theory
2. Matroid examples from finite geometry
3. Affine and projective designs
4. Observations and questions

Observations

- For any k, ℓ there exist a projective Steiner system $S(1, k, k\ell)$, namely a *spread*.
  Hence there exist an affine Steiner system $S(2, k+1, k\ell+1)$.
  This includes ($k = 2$) Steiner triple systems $S(2, 3, 2\ell+1)$ and the "affine q-analog" of the Fano plane $S(2, 3, 7)$.
- Let us examine the affine Steiner system $S(2, 3, 7)$ for $q = 2$.
  This is a family $\mathcal{B}$ of planes in $\mathbf{A}(\mathbb{F}_2^6)$ such that each line is contained in exactly one plane in $\mathcal{B}$.
  How many lines in $\mathbf{A}(\mathbb{F}_2^6)$? Answer: 2016.
  The size of $\mathcal{B}$ is $\frac{1}{6} \cdot 2016 = 16 \cdot 21 = 336$.

Possible application in random network coding

Instead of relaying a linear combination
propagate an affine combination.



$$w = \sum_{i=1}^{n} \lambda_i v_i$$

where $\sum_{i=1}^{n} \lambda_i = 1$

The affine dimension is *submodular*, i.e.,
$\dim(X \vee Y) + \dim(X \wedge Y) \leq \dim X + \dim Y$.
Can be extended to a metric d by $d(X, Y) := \dim(X \vee Y) - \dim X$.

Final remarks

- There is an affine Steiner system $S(2,3,7)$ invariant under the Singer cycle of size 63 and which has 273 parallel classes.
  - Used in [EV11, Lem. 6] to construct a 2-dim. spaces covering code in $\mathrm{Grass}_2(7,3)$ of size 399.
- Is there an affine Steiner system $S(2,3,7)$ which is *skew*, i.e., with no pair of parallel planes?
  - If yes, then a new $(7,3,2)_2$ subspace code of size 336 is found.
  - If no, then the non-existence of the projective q-analog of the Fano plane $S(2,3,7)$ would be proven.

References

- M. K. Bennett, *Affine and projective geometry*, John Wiley & Sons, Inc., New York (1995)
- A. Beutelspacher, U. Rosenbaum, *Projective geometry: from foundations to applications*, Cambridge University Press, Cambridge (1998)
- P. J. Cameron, M. Deza, "Designs and matroids," in: C. J. Colbourn, J. H. Dinitz (eds.), *Handbook of Combinatorial Designs*, CRC Press (2006), 847–852.
- T. Etzion, A. Vardy, *On q-analogs of Steiner systems and covering designs*, Adv. Math. Commun. **5**(2) (2011), 161–176.
- J. Oxley, *Matroid theory*, Second Ed., Oxford University Press, Oxford, 2011.
- H. Whitney, "On the abstract properties of linear dependence," *Amer. J. Math.* **57**(3) (1935), 509–533.