Designs, codes, matroids, and their q-analogues

Relinde Jurrius

University of Neuchâtel, Switzerland

May 5, 2015

Kirkman, 1850:

"Fifteen young ladies in a school walk out three abreast for seven days in succession: it is required to arrange them daily so that no two shall walk twice abreast."

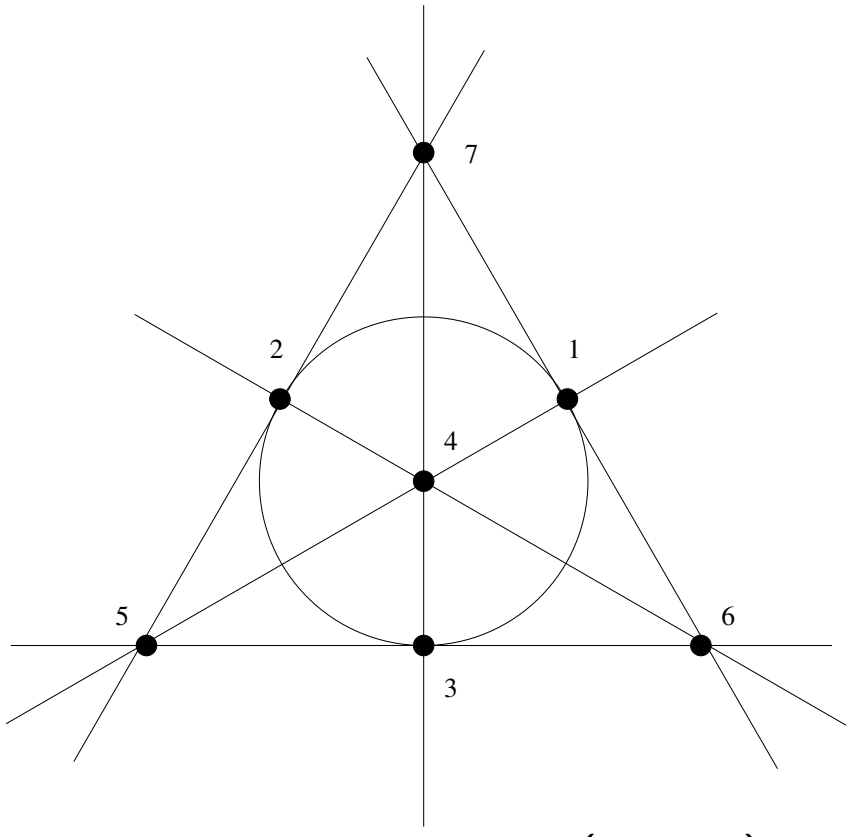
t-(v, k, λ) design: pair $(X, \mathcal{B})$ with

- X set with v elements (points)
- $\mathcal{B}$ family of subsets of X of size k (blocks)
- Every t-tuple of points is contained in exactly λ blocks

Example

The solution to Kirkman's schoolgirl problem is a 2-$(15, 3, 1)$ design.

Example



$$X = \{1, 2, 3, 4, 5, 6, 7\}$$

$$\begin{aligned}\mathcal{B} = \{&\{1, 2, 3\},\\ &\{1, 4, 5\},\\ &\{1, 6, 7\},\\ &\{2, 4, 6\},\\ &\{2, 5, 7\},\\ &\{3, 4, 7\},\\ &\{3, 5, 6\}\}\end{aligned}$$

The Fano plane is a 2-$(7, 3, 1)$ design.

The parameters t, v, k, λ of a design are called admissable if for every $1 \leq s \leq t$, $\binom{k-s}{t-s}$ divides $\lambda\binom{v-s}{t-s}$.

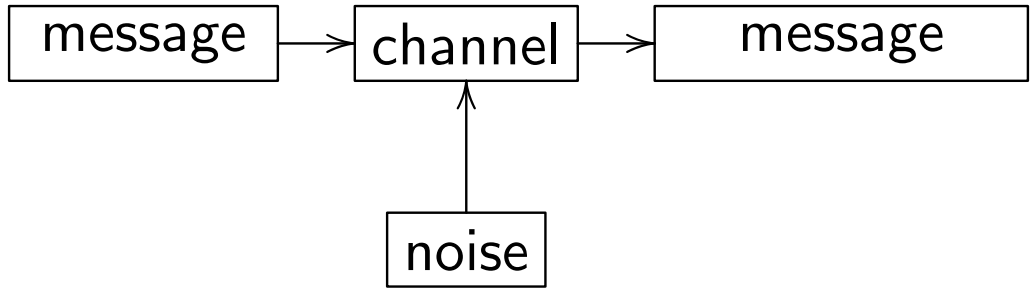
Theorem (Keevash,2014)

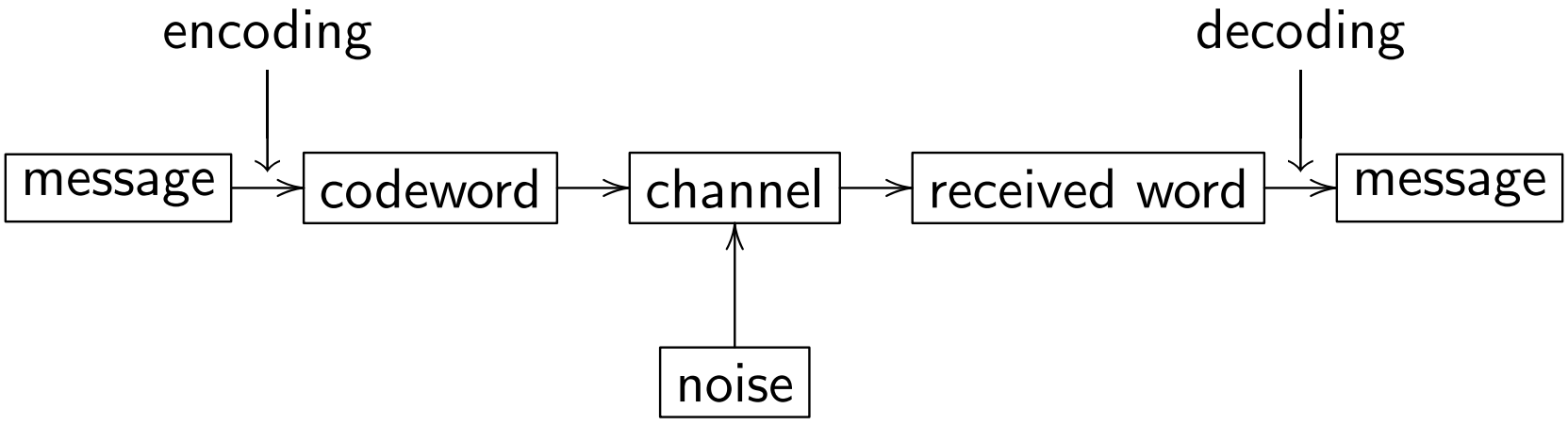
Designs exist for all but finitely many admissable t, k, λ and v big enough.

But: we don't know any designs with $\lambda = 1$ and $t > 5$!

Some research directions:

- (Non)existence, constructions
- Embedding in finite geometry
- Rank of incidence matroid
- Automorphisms
- Links with other combinatorial objects


message
channel
message
noise


encoding
decoding
message
codeword
channel
received word
message
noise

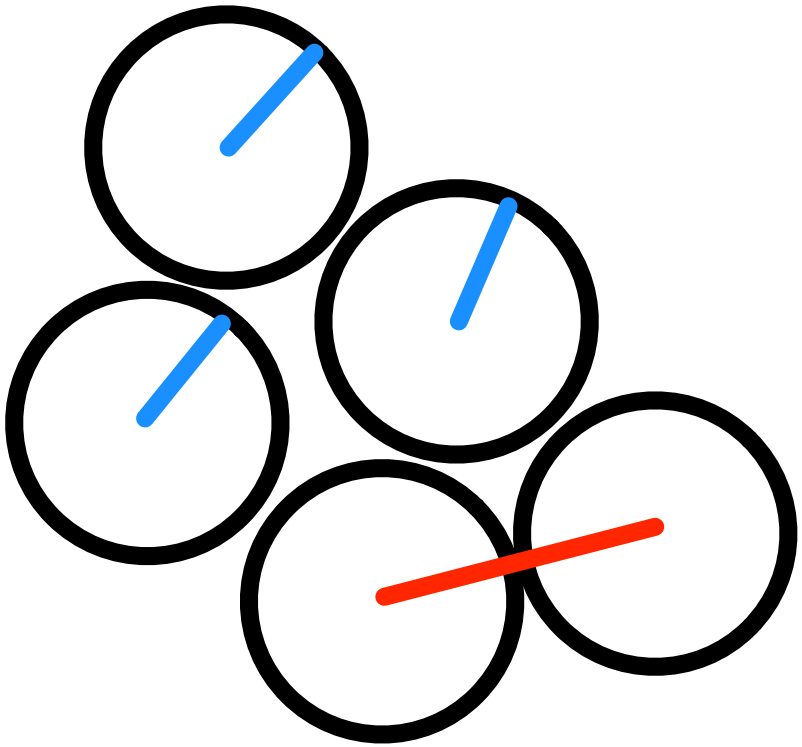
Alphabet $\mathcal{Q}$

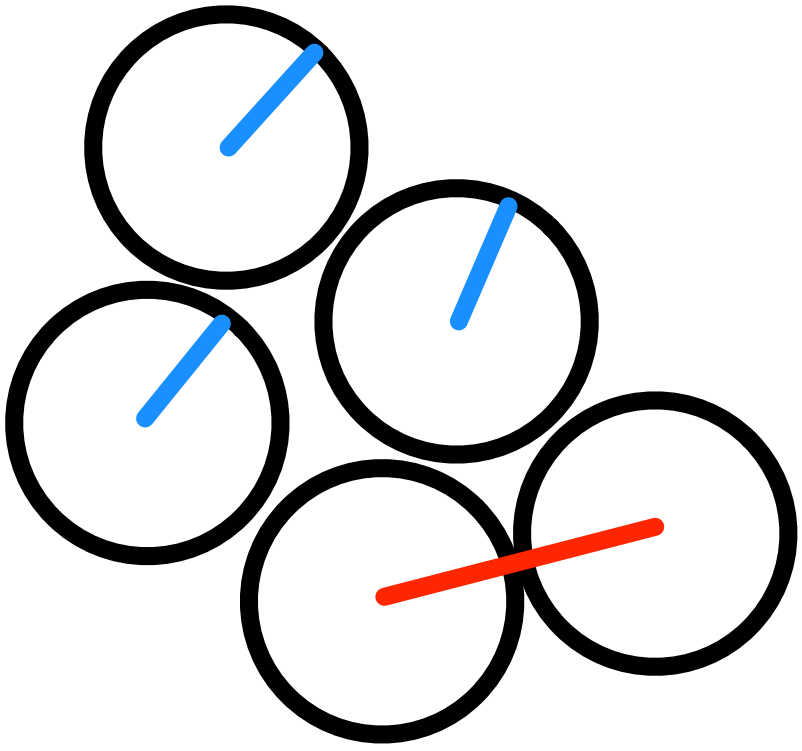
Length n

Hamming metric on $\mathcal{Q}^n$:

$$\begin{aligned} d(x,y) &= \text{number of positions in which vectors differ} \\ &= |\{i \in [n] : x_i \neq y_i\}| \end{aligned}$$

error-correcting code: $C \subseteq \mathcal{Q}^n$





d minimum distance

e error-correcting capacity

$$= \lfloor \frac{d-1}{2} \rfloor$$

Linear code: $C \subseteq \mathbb{F}_q^n$ subspace of dimension k

Generator matrix: rows generate C

Example

The extended Hamming code has generator matrix:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

It has length $n = 8$, dimension $k = 4$ and minimum distance $d = 4$. It can correct 1 error.

Some research directions:

- Given two of n, k, d; optimize the third
- (Non)existence, constructions
- Efficient decoding
- Bounds on the parameters
- Links with other combinatorial objects

Example

The 14 words of weight 4 of the extended Hamming code are the incidence vectors of a 2-$(8, 4, 1)$ design.

In fact, this design is AG$(3, 2)$ and the columns of G give a coordinatization:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Matroid: a pair $(E, \mathcal{I})$ with

- E finite set;
- $\mathcal{I} \subseteq 2^E$ family of subsets of E, the *independent sets*, with:
  (I1) $\emptyset \in \mathcal{I}$
  (I2) If $A \in \mathcal{I}$ and $B \subseteq A$ then $B \in \mathcal{I}$.
  (I3) If $A, B \in \mathcal{I}$ and $|A| > |B|$ then there is an $a \in A \setminus B$ such that $B \cup \{a\} \in \mathcal{I}$.

Examples:

- Set of vectors; independence = linear independence
- Set of edges of a graph; independence = cycle free

Matroids are everywhere: graphs, linear algebra, optimization, tropical geometry, hyperplane arrangements, topology, ...

Some research directions:

- Does a matroid come from a graph?
- Does a matroid come from a set of vectors? Over which field?
- How many matroids are there?
- Study concrete class of matroids
- Links with other combinatorial objects

A matroid is also a pair (E, r) with

- E finite set;
- $r : 2^E \to \mathbb{N}_0$ a function, the *rank function*, with for all $A, B \in E$:

  (r1) $0 \leq r(A) \leq |A|$
  (r2) If $A \subseteq B$ then $r(A) \leq r(B)$.
  (r3) $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$ (semimodular)

$r(A) =$ size of largest independent set contained in A

$\mathcal{I} = \{$subsets whose size is equal to their rank$\}$

A linear code C is a matroid with

$E =$ set of columns of generator matrix

$r(A) =$ rank of submatrix formed by columns of A

Lemma (Tsfasman, Vlăduț, 1991)

$r(A) = \dim C - l(A)$, *where*

$$l(A) = \dim\{\mathbf{c} \in C : c_i = 0 \text{ for all } i \in A\}.$$

A matroid is also a pair $(E, \mathcal{F})$ with

- E finite set;
- $\mathcal{F} \subseteq 2^E$ family of subsets of E, the *flats*, with:

  (F1) $E \subseteq \mathcal{F}$

  (F2) If $A, B \subseteq \mathcal{F}$ then $A \cap B \in \mathcal{F}$.

  (F3) If $F \in \mathcal{F}$ and $\{F_1, \ldots, F_k\}$ the set of flats that cover F then $\{F_1 - F, \ldots, F_k - F\}$ partition $E - F$.

$F \subseteq E$ is a flat if $r(F \cap \{x\}) > r(F)$ for all x not in F

A t-$(v, k, 1)$ design $(X, \mathcal{B})$ is a matroid with

$E = X$ (set of points)

$\mathcal{F} = \{X$, all blocks in $\mathcal{B}$, and all their intersections$\}$

Matroids whose flats of the same rank have the same size are called *perfect matroid designs*.

Summary so far:

- Designs, codes and matroids were introduced
- Designs give (good) codes
- Codes are matroids
- Designs with $\lambda = 1$ are matroids

Commercial break

Commercial break

Put in your calendar:

Saturday March 12, 2016

Open doors day Faculty of Science

I will need your help!

q-analogue: finite set $\longrightarrow$ finite vector space over $\mathbb{F}_q$

Example

$$\binom{n}{k} = \text{number of sets of size } k \text{ contained in set of size } n$$

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \text{number of } k\text{-dim subspaces of } n\text{-dim vector space over } \mathbb{F}_q$$

$$= \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}$$

finite set	finite space $\mathbb{F}_q^n$
element	1-dim subspace
size	dimension
n	$\frac{q^n-1}{q-1}$
intersection	intersection
union	sum
complement	quotient space

From q-analogue to 'normal': let $q \to 1$.

Candidates for complement A^c of $A \subseteq E$:

- All vectors outside A
  But: not a space
- Orthogonal complement
  But: $A \cap A^\perp$ can be nontrivial
- Quotient space E/A
  But: changes ambient space
- Subspace such that $A \oplus A^c = E$
  But: not unique

t-$(v, k, \lambda; q)$ q-design: pair $(X, \mathcal{B})$ with

- X v-dim vectorspace over $\mathbb{F}_q$
- $\mathcal{B}$ family of k-dim subspaces of X (blocks)
- Every t-dim subspace is contained in exactly λ blocks

Example

$t = 1$, $\lambda = 1$: spread

The parameters t, v, k, λ, q of a design are called admissable if for every $1 \leq s \leq t$, $\begin{bmatrix} k-s \\ t-s \end{bmatrix}_q$ divides $\lambda \begin{bmatrix} v-s \\ t-s \end{bmatrix}_q$.

Theorem (Fazeli, Lovett, Vardy,2014)

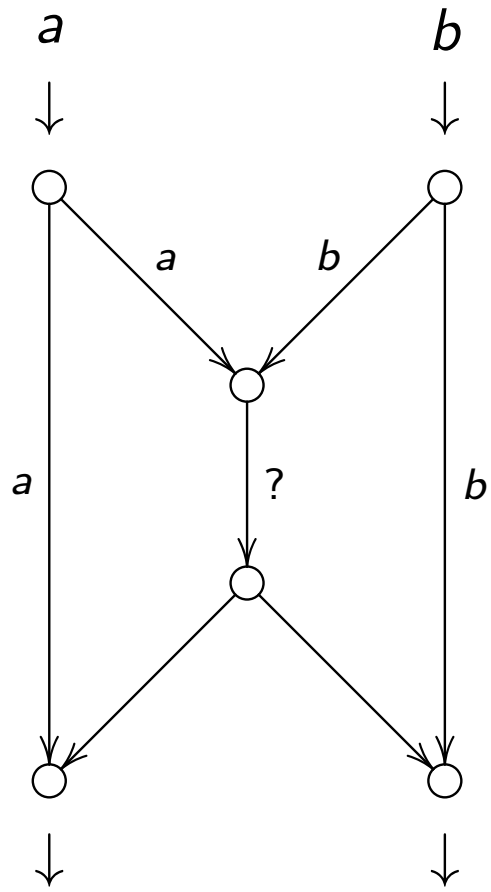
"Nontrivial t-designs over finite fields exist for all t"

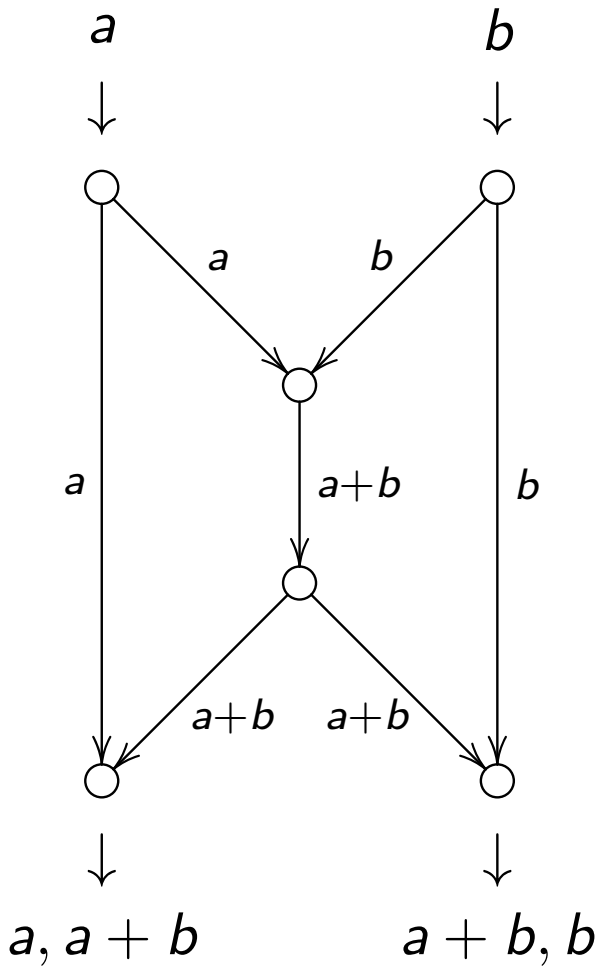
But: we don't know any designs with $t > 3$!

$\lambda = 1$: long conjectured to only exist for $t = 1$

Theorem (Braun, Etzion, Östergård, Vardy, Wasserman, 2014)
There exist 2-$(13, 3, 1; 2)$ *designs.*

Example
Existence of q-analogue of the Fano plane 2-$(7, 3, 1; q)$ is unknown. It has 381 blocks.


a
b
a
b
a
?
b



Idea: send (rows of) matrices instead of vectors

Better idea: send (bases of) subspaces instead of matrices

Codewords are vectors:

- 'Ordinary' error-correcting codes

Codewords are matrices:

- Rank metric codes
- q-analogue of 'ordinary' codes

Codewords are subspaces:

- Subspace codes
- Constant dimension, constant weight: q-design

q-Matroid: a pair $(E, \mathcal{I})$ with

- E finite dimensional vector space;
- $\mathcal{I}$ family of subspaces of E, the *independent spaces*, with:

  (I1) $\mathbf{0} \in \mathcal{I}$

  (I2) If $A \in \mathcal{I}$ and $B \subseteq A$ then $B \in \mathcal{I}$.

  (I3) If $A, B \in \mathcal{I}$ and $\dim A > \dim B$ then there is a 1-dimensional subspace $a \subseteq A$, $a \nsubseteq B$ such that $B + a \in \mathcal{I}$.

A q-matroid is also a pair (E, r) with

- E finite dimensional vector space;
- $r : \{\text{subspaces of } E \to \mathbb{N}_0$ a function, the *rank function*, with for all $A, B \in E$:

  (r1) $0 \leq r(A) \leq \dim A$
  (r2) If $A \subseteq B$ then $r(A) \leq r(B)$.
  (r3) $r(A + B) + r(A \cap B) \leq r(A) + r(B)$ (semimodular)

$r(A) =$ dimension of largest independent space contained in A

$\mathcal{I} = \{\text{subspaces whose dimension is equal to their rank}\}$

For 'normal' codes:

Lemma (Tsfasman, Vlădut, 1991)
$r(A) = \dim C - l(A)$, *where*

$$l(A) = \dim\{\mathbf{c} \in C : c_i = 0 \text{ for all } i \in A\}.$$

For rank metric codes:

Theorem (J., Pellikaan)
Let $r(A) = \dim C - l(A)$ *with*

$$l(A) = \dim\{M \in C : \mathit{rowsp}(M) \subseteq A^{\perp}\}.$$

Then $r(A)$ *is the rank function of a q-matroid.*

q-Analogue of perfect matroid design?

Easy part: $F \subseteq E$ is a flat if $r(F + x) > r(F)$ for all 1-dimensional subspaces x not in F

Difficult part: recall a 'normal' matroid is a pair $(E, \mathcal{F})$ with

- E finite set;
- $\mathcal{F} \subseteq 2^E$ family of subsets of E, the *flats*, with:

  (F1) $E \subseteq \mathcal{F}$

  (F2) If $A, B \subseteq \mathcal{F}$ then $A \cap B \in \mathcal{F}$.

  (F3) If $F \in \mathcal{F}$ and $\{F_1, \ldots, F_k\}$ the set of flats that cover F then $\{F_1 - F, \ldots, F_k - F\}$ partition $E - F$.

Some research directions (i.e., my to do-list):

- Different (but equivalent) definitions
- New q-matroids from old
- Polynomial links between rank metric codes and q-matroids
- q-Analogue of graph?
- q-Analogue of perfect matroid design