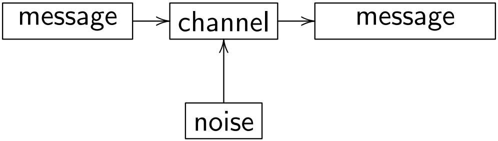
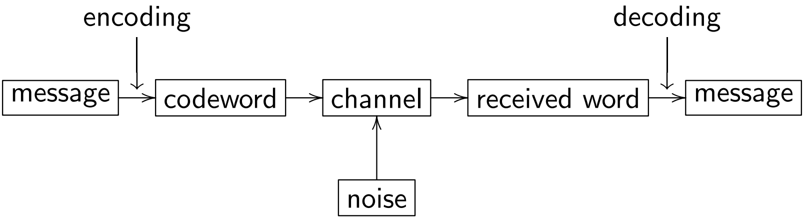
# Codes and related combinatorial structures

Relinde Jurrius
(joint work with Henry Crapo, Ruud Pellikaan)

The Netherlands Defence Academy

PhD seminar, UGent
February 22, 2018


message
channel
message
noise



encoding
decoding
message
codeword
channel
received word
message
noise

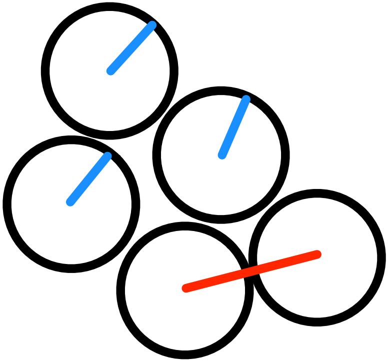
Alphabet $\mathcal{Q}$

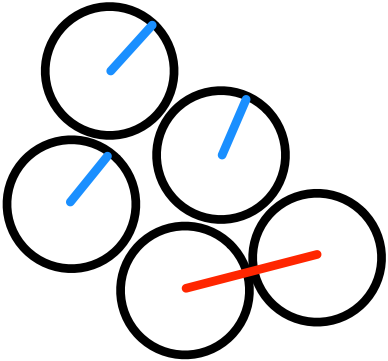
Length $n$

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

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

A linear code $C$ is a subspace of $\mathbb{F}_q^n$.

- $n$ length of the code
- $k$ dimension of the code

A $k \times n$ matrix whose rows span $C$ is called a generator matrix.

## Running example

The $[7, 4]$ Hamming code over $\mathbb{F}_2$ has generator matrix

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

It has length $n = 7$, dimension $k = 4$ and minimum distance $d = 3$. 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

$C$ linear code

$$\mathrm{supp}(\mathbf{c}) = \text{ coordinates of } \mathbf{c} \text{ that are non-zero}$$
$$\mathrm{wt}_H(\mathbf{c}) = \text{ size of support}$$

Weight enumerator

$$W_C(X,Y) = \sum_{w=0}^{n} A_w X^{n-w} Y^w$$

with $A_w =$ number of words of weight $w$.

## Example

Hamming code generated by $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$.

Some words and weights:

| $\mathbf{c}$ | $\mathrm{supp}(\mathbf{c})$ | $\mathrm{wt}_H(\mathbf{c})$ |
|---|---|---|
| $\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ | $\emptyset$ | 0 |
| $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$ | $\{1, 5, 6\}$ | 3 |
| $\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$ | $\{2, 3, 4, 7\}$ | 4 |

The weight enumerator is equal to

$$W_C(X, Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7.$$

$J$ subset of $[n]$

$$C(J) = \{\mathbf{c} \in C : \mathrm{supp}(\mathbf{c}) \subseteq J^c\}$$

Lemma

*$C(J)$ is a subspace of $\mathbb{F}_q^n$*

$$\ell(J) = \dim_{\mathbb{F}_q} C(J)$$

Theorem

*$\ell(J)$ gives a nice formula for the weight enumerator.*

Example

Hamming code generated by $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$.

Some calculations of $C(J)$:

| $J$ | $J^c$ | $C(J)$ |
|---|---|---|
| $[n]$ | $\emptyset$ | $\mathbf{0}$ |
| size $= 5$ | size $= 2$ | $\mathbf{0}$ |
| $\{1, 5, 6\}$ | $\{2, 3, 4, 7\}$ | $\left\langle \begin{matrix} 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{matrix} \right\rangle$ |
| $\{1\}$ | $\{2, 3, 4, 5, 6, 7\}$ | $\left\langle \begin{matrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{matrix} \right\rangle$ |

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 $B \cup \{a\} \in \mathcal{I}$.

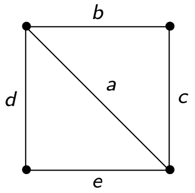
Examples:

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

Example

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

Example




But: most matroids don't come from a matrix or graph.

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)

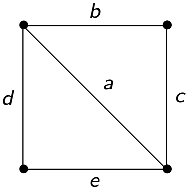
$r(A) =$ size of largest independent set contained in $A$

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

Example

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

Example



Fact: a linear code gives a matroid with

$E =$ index set for columns of generator matrix

$r(J) =$ dimension of subspace spanned by vectors indexed by $J$

Recall: $\ell(J) = \dim\{\mathbf{c} \in C : \mathrm{supp}(\mathbf{c}) \subseteq J^c\}$

Theorem

$r(J) = \dim C - \ell(J)$

Idea of proof: $0 \to C(J) \to C \to C_J \to 0$ is an exact sequence.

# Comercial break

Source: Ministry of Defence

# $q$-Analogues

Finite set $\longrightarrow$ finite dimensional vectorspace over $\mathbb{F}_q$

Example

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

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

# $q$-Analogues

Example

$t$-$(v, k, \lambda)$ 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 $\lambda$ blocks

$t$-$(v, k, \lambda; q)$ $q$-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 $\lambda$ blocks

# $q$-Analogues

| 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 | ? |

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

Candidates for complement $A^c$ of $A \subseteq \mathbb{F}_q^n$:

- All vectors outside $A$

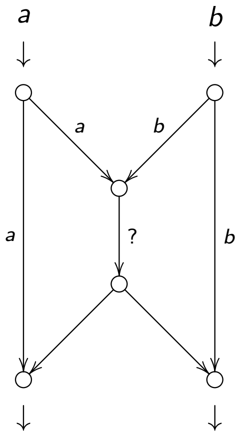
  But: not a space
- Orthogonal complement

  But: $A \cap A^\perp$ can be nontrivial
- Quotient space $\mathbb{F}_q^n / A$

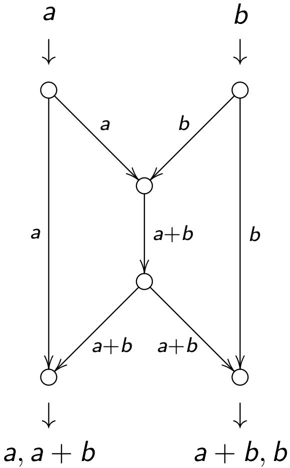
  But: changes ambient space
- Subspace such that $A \oplus A^c = \mathbb{F}_q^n$

  But: not unique

# Network coding



# Network coding




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:

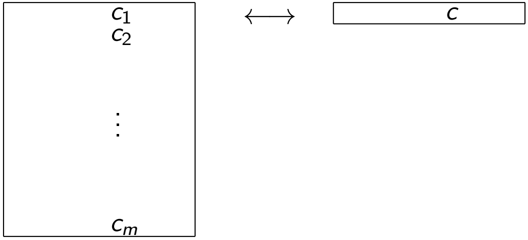
Subspace codes

Constant dimension, constant weight: $q$-design

# Rank metric codes

$\mathbb{F}_{q^m}/\mathbb{F}_q$ finite field extension with basis $\alpha_1, \ldots, \alpha_m$.

Write $c = c_1\alpha_1 + \cdots + c_m\alpha_m$.




$m(\mathbf{x}) \in \mathbb{F}_q^{m\times n}$ $\qquad$ $\mathbf{x} \in \mathbb{F}_{q^m}^n$

Rank metric code is subspace of $\mathbb{F}_{q^m}^n \to$ subspace of $\mathbb{F}_q^{m\times n}$.

## Running example

Let $\mathbb{F}_8/\mathbb{F}_2$ with basis $(1, \alpha, \alpha^2)$, where $\alpha^3 = \alpha + 1$.
Let $C$ be the code generated by

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

Some words and matrices:

$$\begin{array}{cccc} \mathbf{c} & (0,0,0,0) & (1,\alpha,0,0) & (1,\alpha^2,\alpha^5,0) \\ m(\mathbf{c}) & \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

$C$ linear code

$$\mathrm{supp}(\mathbf{c}) = \text{ coordinates of } \mathbf{c} \text{ that are non-zero}$$

$$\mathrm{wt}_H(\mathbf{c}) = \text{ size of support}$$

Weight enumerator

$$W_C(X, Y) = \sum_{w=0}^{n} A_w X^{n-w} Y^w$$

with $A_w$ = number of words of weight $w$.

$C$ rank metric code

$\mathrm{Rsupp}(\mathbf{c}) =$ row space of $m(\mathbf{c})$

$\mathrm{wt}_R(\mathbf{c}) =$ dimension of support

Rank weight enumerator

$$W_C^R(X, Y) = \sum_{w=0}^{n} A_w^R X^{n-w} Y^w$$

with $A_w^R =$ number of words of rank weight $w$.

Example

$C$ in $\mathbb{F}_8/\mathbb{F}_2$ generated by $G = \begin{pmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \end{pmatrix}$.

Some words and weights:

$$\begin{array}{llll}
\mathbf{c} & (0,0,0,0) & (1,\alpha,0,0) & (1,\alpha^2,\alpha^5,0) \\
m(\mathbf{c}) & \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \\
\mathrm{Rsupp}(\mathbf{c}) & \mathbf{0} & \left\langle \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{matrix} \right\rangle & \left\langle \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{matrix} \right\rangle \\
\mathrm{wt}_R(\mathbf{c}) & 0 & 2 & 3
\end{array}$$

There are no words of weight 1 or weight 4.

$J$ subset of $[n]$

$$C(J) = \{\mathbf{c} \in C : \mathrm{supp}(\mathbf{c}) \subseteq J^c\}$$

Lemma

*$C(J)$ is a subspace of $\mathbb{F}_q^n$*

$$\ell(J) = \dim_{\mathbb{F}_q} C(J)$$

Theorem

*$\ell(J)$ gives a nice formula for the weight enumerator.*

$J$ subspace of $\mathbb{F}_q^n$

$$C(J) = \{\mathbf{c} \in C : \mathrm{Rsupp}(\mathbf{c}) \subseteq J^{\perp}\}$$

Lemma
*$C(J)$ is a subspace of $\mathbb{F}_{q^m}^n$*

$$\ell(J) = \dim_{\mathbb{F}_{q^m}} C(J)$$

Theorem
*$\ell(J)$ gives a nice formula for the rank weight enumerator.*

Example

$C$ in $\mathbb{F}_8/\mathbb{F}_2$ generated by $G = \begin{pmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \end{pmatrix}$.

Some calculations of $C(J)$:

| $J$ | $J^\perp$ | $C(J)$ |
|---|---|---|
| $\mathbb{F}_2^4$ | $\mathbf{0}$ | $\mathbf{0}$ |
| $\dim = 3$ | $\dim = 1$ | $\mathbf{0}$ |
| $\left\langle \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{matrix} \right\rangle$ | $\left\langle \begin{matrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} \right\rangle$ | $\mathbf{0}$ |
| $\left\langle \begin{matrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} \right\rangle$ | $\left\langle \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{matrix} \right\rangle$ | $\left\langle \begin{matrix} 1 & \alpha & 0 & 0 \end{matrix} \right\rangle$ |

If $\dim J = 2$ and $J^\perp \not\subseteq \left\langle \begin{matrix} 0 & 0 & 0 & 1 \end{matrix} \right\rangle^\perp$ then $C(J) = \mathbf{0}$.

Recall: for linear codes and their associated matroids, we have proven $r(J) = \dim C - \ell(J)$.

Theorem

*Let $r(J) = \dim C - \ell(J)$ for a rank metric code $C$. Then $r(J)$ satisfies:*

(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)*

This leads to the definition of the rank function of a $q$-matroid.

$q$-Matroid: 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 $A, B \subseteq E$:
  - (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)

Example

$C$ in $\mathbb{F}_8/\mathbb{F}_2$ generated by $G = \begin{pmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \end{pmatrix}$.

Some calculations of $r(J)$:

| $J$ | $C(J)$ | $r(J)$ |
|---|---|---|
| $\mathbb{F}_2^4$ | $\mathbf{0}$ | 2 |
| $\dim = 3$ | $\mathbf{0}$ | 2 |
| $\left\langle \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{matrix} \right\rangle$ | $\mathbf{0}$ | 2 |
| $\left\langle \begin{matrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} \right\rangle$ | $\langle \begin{matrix} 1 & \alpha & 0 & 0 \end{matrix} \rangle$ | 1 |

If $\dim J = 2$ and $J^\perp \not\subseteq \langle \begin{matrix} 0 & 0 & 0 & 1 \end{matrix} \rangle^\perp$ then $r(J) = 2$.

These are exactly the bases of the $q$-matroid.

Theorem

*A q-matroid is 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 $J \in \mathcal{I}$ and $I \subseteq J$, then $I \in \mathcal{I}$.*
  - (I3) *If $I, J \in \mathcal{I}$ with $\dim I < \dim J$, then there is some 1-dimensional subspace $x \subseteq J$, $x \not\subseteq I$ with $I + x \in \mathcal{I}$.*
  - (I4) *Let $A, B \subseteq E$ and let $I, J$ be maximal independent subspaces of $A$ and $B$, respectively. Then there is a maximal independent subspace of $A + B$ that is contained in $I + J$.*

Note the extra axiom!

Other things that need a $q$-analogue:

- More axiom sets for matroids
- Relation between weight enumerator and Tutte polynomial
- Perfect matroid designs
- Graphs (??)

- How about rank metric cods that are not $\mathbb{F}_{q^m}$-linear?