What is the rank-metric equivalent of a binary code?

Relinde Jurrius

Netherlands Defence Academy
Utrecht University

Open Problems in Rank-Metric Codes
February 24, 2026

What is the rank-metric equivalent of a binary code?

Answer from a computer scientist: just take a rank-metric code over $\mathbb{F}_2$, I guess?

Answer from a combinatorialist: what exactly do you mean?

Why study binary codes?

Answer from a computer scientist: computers work with zeros and ones, so $\mathbb{F}_2$ (and maybe a field extension) is enough.

Answer from a combinatorialist: the incidence matrix of my favourite combinatorial object generates a binary code, and I can study this code using combinatorics. Examples: graph, block design, incidence geometry, ...

Taking a step back: matroids

Definition

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

- E finite set;
- $\mathcal{I}$ family of subsets of E, the *independent sets*, with:
  - (I1) $\mathcal{I} \neq \emptyset$.
  - (I2) If $J \in \mathcal{I}$ and $I \subseteq J$, then $I \in \mathcal{I}$.
  - (I3) If $I, J \in \mathcal{I}$ with $|I| < |J|$, then there is some $x \in J \setminus I$ with $I \cup \{x\} \in \mathcal{I}$.

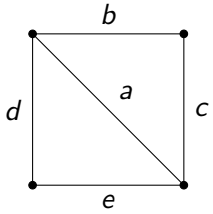
Example

The points in a projective system form a matroid, where independent means linearly independent.

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

Example

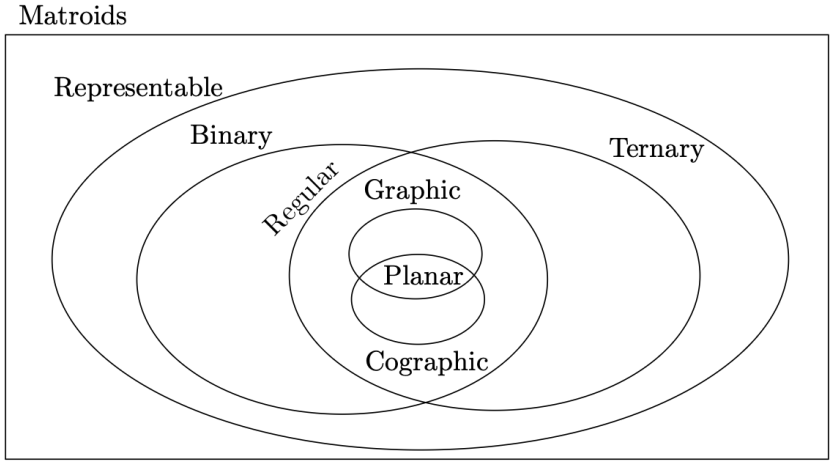
The edges of a graph form a matroid, where independent means cycle-free.



Matroids generalise both graphs and projective systems (i.e., codes).

A matroid coming from a projective system is called a *representable* matroid.

Binary matroids are representable over $\mathbb{F}_2$. They generalise matroids from (the incidence matrices of) graphs.



James Oxley, *Matroid Theory*, page 211

There are many equivalent ways to define a binary matroid:

- it is representable over $\mathbb{F}_2$;
- it has no $U_{2,4}$ minor (that is: no four points on a line);
- the intersection of a circuit and a cocircuit has even cardinality;
- the symmetric difference of two circuits is the disjoint union of circuits;
- ...

So. . . how do we go to rank-metric codes from here?

q-Analogues in combinatorics

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

Example

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

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

q-Analogues in combinatorics

lattice	Boolean	subspace lattice of $\mathbb{F}_q^n$
atom	element	1-dim subspace
height	size	dimension
# atoms	n	$\frac{q^n-1}{q-1}$
meet $\wedge$	intersection	intersection
join $\vee$	union	sum

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

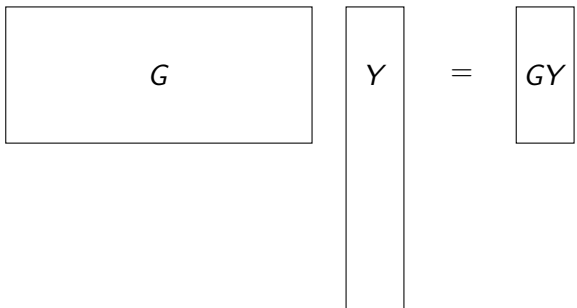
Definition

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) $\mathcal{I} \neq \emptyset$.
  - (I2) If $J \in \mathcal{I}$ and $I \subseteq J$, then $I \in \mathcal{I}$.
  - (nI3) For all $I, J \in \mathcal{I}$ satisfying $\dim I < \dim J$, there exists a codimension 1 subspace $X \subseteq E$ with $I \subseteq X$, $J \not\subseteq X$ such that $I + x \in \mathcal{I}$ for all 1-dimensional $x \subseteq E$, $x \not\subseteq X$.

Example

Let $E = \mathbb{F}_q^n$ and G be a matrix over $\mathbb{F}_{q^m}$ (i.e., an $\mathbb{F}_{q^m}$-linear rank-metric code).
Let $A \subseteq E$ and Y a matrix whose columns span A.



Call A independent if $\dim(A) = \mathrm{rk}(GY)$. Then $(E, \mathcal{I})$ is a q-matroid.

Example

Let $E = \mathbb{F}_2^4$ and $G = \begin{bmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \end{bmatrix}$ over $\mathbb{F}_8$.

$$\begin{bmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \text{so } \langle 0001 \rangle \text{ is dependent.}$$

$$\begin{bmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & \alpha \\ \alpha & 1 \end{bmatrix}, \quad \text{so } A \text{ is independent.}$$

A q-matroid coming from a q-system is called *representable*.

What is the q-analogue of "representable over $\mathbb{F}_2$"?
(Or: of some other property that defines a binary matroid?)

Inspiration: a q-analogue of a graph?

Warning!

This is where the handwaiving starts.

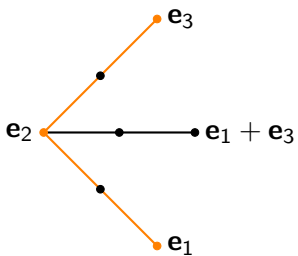
Definition

Let $V = \mathbb{F}_q^v$ and let E be a set of 2-dimensional subspaces of V, the *edges*. Then (V, E) is a q-**ary graph** if for all $c_1, c_2 \in \mathbb{F}_q$:

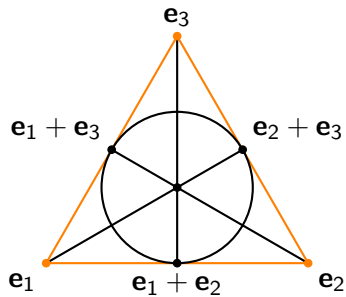
If $\langle \mathbf{x}, \mathbf{y_1} \rangle$ *and* $\langle \mathbf{x}, \mathbf{y_2} \rangle$ *are (adjecent) edges, then* $\langle \mathbf{x}, c_1\mathbf{y_1} + c_2\mathbf{y_2} \rangle$ *is an edge.*

In other words: neighbourhoods are spaces.

Example



q-ary P_2 in $\mathbb{F}_2^3$



q-ary C_3 in $\mathbb{F}_2^3$

Incidence matrix of a graph: matrix over $\mathbb{F}_q$ (usually $\mathbb{F}_2$) with v rows such that

- columns $\leftrightarrow$ edges;
- Hamming support $=$ edge (as a set of vertices);
- so: Hamming weight $= 2$;
- orthogonal to $\begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix}^{\mathsf{T}}$ (full Hamming weight vector).

Incidence matrix of a q-ary graph: matrix over $\mathbb{F}_{q^v} = \mathbb{F}_q[\alpha]$ with v rows such that

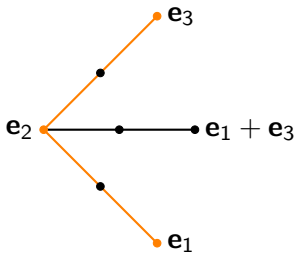
- columns $\leftrightarrow$ edges;
- rank support $=$ edge (as a space);
- so: rank weight $= 2$;
- orthogonal to $\begin{bmatrix} 1 & \alpha & \cdots & \alpha^{v-1} \end{bmatrix}^{\mathsf{T}}$ (full rank weight vector);
- behaves nicely with the q-ary graph property.

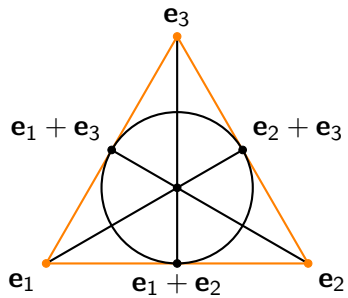
Theorem

Let $\langle \mathbf{x}, \mathbf{y}_1 \rangle, \ldots, \langle \mathbf{x}, \mathbf{y}_d \rangle$ *be edges through the same vertex. Fix a representation* $\mathbf{v}_1$ *of the edge* $\langle \mathbf{x}, \mathbf{y}_1 \rangle$*. Then there exist unique representations* $\mathbf{v}_2, \ldots, \mathbf{v}_d$ *of the edges* $\langle \mathbf{x}, \mathbf{y}_2 \rangle, \ldots, \langle \mathbf{x}, \mathbf{y}_d \rangle$ *such that for any* $\lambda_1, \ldots, \lambda_d \in \mathbb{F}_q$ *the vector* $\mathbf{v}_{d+1} := \lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 + \cdots + \lambda_d \mathbf{v}_d$ *is a representation of the edge* $\langle \mathbf{x}, \sum_{i=1}^{d} \lambda_i \mathbf{y}_i \rangle$.

Proof: constructive, by linear algebra.

Example





$$\begin{bmatrix} \alpha & 0 & \alpha \\ 1 & \alpha^2 & \alpha^6 \\ 0 & \alpha & \alpha \end{bmatrix}$$

$$\begin{bmatrix} \alpha & 0 & \alpha^2 & \alpha & \alpha^4 & \alpha^2 & \alpha^4 \\ 1 & \alpha^2 & 0 & \alpha^6 & 1 & \alpha^2 & \alpha^6 \\ 0 & \alpha & 1 & \alpha & 1 & \alpha^3 & \alpha^3 \end{bmatrix}$$

Theorem

For every q-ary graph, fixing the representation of one edge fixes a representation for all other edges up to a scalar in $\mathbb{F}_q^*$.
Starting with a different representation for the first edge, or with a different first edge, will multiply the whole incidence matrix with a scalar $\mathbb{F}_{q^v}^*$.

So: different incidence matrices give isomorphic q-matroids.

Conjecture:

The q-analogue of a 0-1 incidence vector of a set is a vector over $\mathbb{F}_{q^m}$ with a given subspace as support. We need extra properties to make this choice unique up to a scalar in $\mathbb{F}_q^*$.

(Now generalise this idea to find the q-analogue of a binary code!)