Symmetries Of Rank-Metric Codes

Dan Hawtin – University of Rijeka, Croatia

NORCOM 2025

This work was supported by the Croatian Science Foundation under the project number HRZZ–IP–2022–10–4571.

Codes in graphs

Definition

A code C in a graph Γ is a subset of the vertex set of Γ.

Book advertisement:

- Completely regular codes in distance-regular graphs. Editors: M. Shi and P. Solé. Chapman and Hall/CRC, 2025.
- Contributed chapter: D.R.H. and C.E. Praeger, Group actions on codes in graphs. https://arxiv.org/abs/2407.09803.

Bilinear forms graphs

Definition

The vertex-set of the bilinear forms graph $H_q(m,n)$ is the set of bilinear forms $\mathbb{F}_q^m \times \mathbb{F}_q^n \to \mathbb{F}_q$ where f,g are adjacent when $\operatorname{rank}(f-g)=1$.

Alternative descriptions of vertex-set:

- Matrices: $M_{m\times n}(q)$.
- Linear maps: $\mathbb{F}_q^m \to \mathbb{F}_q^n$.
- Tensors: $\mathbb{F}_q^m \otimes \mathbb{F}_q^n$.

$H_q(m,n)$ is the q-analogue of the Hamming graph.

Rank-metric codes

The metric given by $H_q(m, n)$ is known as the rank-metric, and codes in $H_q(m, n)$ are called rank-metric codes.

Important parameters:

- minimum distance δ of C
  – smallest distance between distinct codewords
- covering radius ρ of C
  – distance to furthest vertex from C
- error-correction capacity $e = \lfloor (\delta - 1)/2 \rfloor$ of C
  – largest radius of disjoint balls centred at codewords

Rank-metric codes

Collection of surveys:

- Network coding and subspace designs, Greferath, M., Pavčević, M.O., Silberstein, N. and Vázquez-Castro, M.A. eds. Springer, 2018.

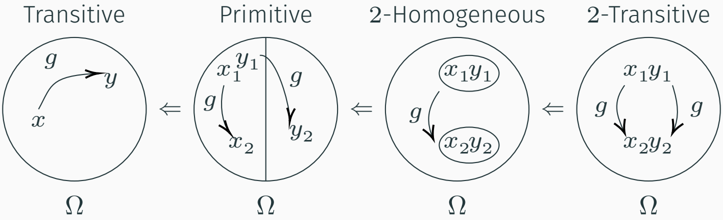
Maximum rank-distance (MRD) codes satisfy a 'Singleton-like' bound.

- Delsarte (1978) introduced a class of MRD codes reintroduced by Gabidulin (1985) – several generalisations of these studied.
- MRD codes have connections to *semifields* and *skew polynomial algebras*.

Permutation Groups

If G is a group and Ω a set with $G \leq \mathrm{Sym}(\Omega)$, then G is

- transitive if Ω is a G-orbit
- primitive if G preserves no non-trivial partition of Ω
- 2-homogeneous if G acts transitively on the set of 2-subsets of Ω
- 2-transitive if G acts transitively on the set of pairs of distinct elements of Ω



Automorphsims

Theorem

The automorphism group of $H_q(m,n)$ is

$$G = T.((\mathrm{GL}_m(q) \circ \mathrm{GL}_n(q)).\,\mathrm{Aut}(\mathbb{F}_q))$$

when $m \neq n$, or $G.2$ when $m = n$, where $T = \mathbb{F}_q^{m\times n}$.

Generators (matrix model):

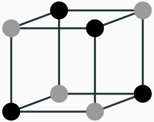
- Translations $t_A : M \mapsto M + A$ for any $A \in M_{m\times n}(q)$.
- Column operations.
- Row operations.
- Field automorphisms.
- Transpose map (for $m = n$).

$H_q(m,n)$ is distance-transitive.

Code automorphisms

Definition

The automorphism group $\mathrm{Aut}(C)$ of a code is its set-wise stabiliser inside $\mathrm{Aut}(\Gamma)$.



Example

Let C be a maximum independent set in $\Gamma = H(3,2)$

- Interchanging pairs of vertices on vertical edges is in $\mathrm{Aut}(\Gamma)$ but not in $\mathrm{Aut}(C)$
- A $2\pi/3$ rotation about a long diagonal is in $\mathrm{Aut}(C)$

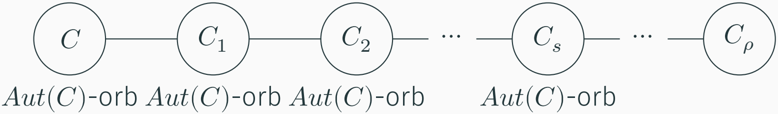
s-Neighbour-transitive codes

Distance partition $\{C = C_0, C_1, \dots, C_\rho\}$ of $V(\Gamma)$ wrt C

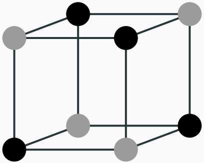
Definition

A code C is

1. s-neighbour-transitive (s-NT) if $\mathrm{Aut}(C)$ acts transitively on the set of i-neighbours C_i for each $i \le s$
2. completely transitive (CT) if C is ρ-NT



A neighbour-transitive code



Example

Let C be the set of black vertices

- Then C_1 is the set of grey vertices
- Rotations about long diagonals generate a group acting transitively on each of C and C_1
- Hence C is NT and CT

Symmetry of codes

- Perfect codes 1973 – Tietäväinen, and Zinoviev and Leontiev, independently classified parameters of non-trivial perfect codes in Hamming graphs over finite fields.
- Uniformly packed codes – Introduced by Semakov, Zinoviev, and Zaitsev (1971).
- s-Regular and completely regular codes – Introduced in association schemes by Delsarte (1973).
- CT codes – Solé (1987) for binary linear codes, Godsil and Praeger (1988) in Johnson graphs, Giudici and Praeger (2000) in Hamming graphs.
- NT codes – PhD thesis of Gillespie (2011) for $s = 1$ in Hamming graphs.

Linearised polynomials and Gabidulin codes

Linearised polynomials have the form:

$$f(x) = a_0 x + a_1 x^q + \cdots + a_k x^{q^k}.$$

If $f \in \mathbb{F}_{q^n}[x]$ then $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ an $\mathbb{F}_q$-linear transformation.

Definition

The Gabidulin code $\mathcal{G}_{n,k,s}$ (with $\gcd(s,n) = 1$) in $H_q(n,n)$ is

$$\left\langle x, x^{q^s}, \dots, x^{q^{s(k-1)}} \right\rangle_{\mathbb{F}_{q^n}}.$$

$\mathcal{G}_{n,k,s}$ is MRD and NT, being invariant under $\mathbb{F}_{q^n}^\times \circ \mathbb{F}_{q^n}^\times$.

NT codes with $m \neq n$

Let $t = \gcd(m, n)$. Using the trace map $\mathrm{tr} : \mathbb{F}_{q^m} \to \mathbb{F}_{q^t}$ we can construct NT codes with $m \neq n$:

$$\mathrm{tr}(x) = x + x^{q^t} + \cdots + x^{q^{t(m/t-1)}}.$$

Proposition

For $k < t$, the following code is NT in $H_q(m, n)$.

$$\left\langle \mathrm{tr}(x), \mathrm{tr}(x^q), \ldots, \mathrm{tr}(x^{q^{k-1}}) \right\rangle_{\mathbb{F}_{q^n}},$$

and is invariant under $\mathbb{F}_{q^m}^\times \circ \mathbb{F}_{q^n}^\times$.

A useful lemma

It's often useful to consider the local action at a codeword:

Lemma

Let C be a code with error-correction capacity $e \geq 1$ in a graph Γ, let $\alpha \in C$, and let $1 \leq s \leq e$. Then the following are equivalent.

(1) C is s-NT.

(2) $\mathrm{Aut}(C)$ acts transitively on C and, for each $i \in \{1, \dots, s\}$, the stabiliser $\mathrm{Aut}(C)_\alpha$ is transitive on $\Gamma_i(\alpha)$.

Transitive projective groups

A transitive linear group is a subgroup of $\mathrm{GL}_n(q)$ acting transitively on $\mathbb{F}_q^n \setminus \{0\}$. These were classified by Hering and Huppert.

Giudici, Glasby and Praeger (2023) classified linear groups acting transitively on k-spaces.

By considering the action on the row-space and column-space of the rank-2 matrices in $M_{m\times n}(q)$, we were able to show:

Theorem (H–Praeger 2025+)

If C is a 2-NT code in $H_q(m,n)$ then $\delta \leq 4$.

Characterisation result

Recall that $T = \mathbb{F}_q^{m\times n}$ and

$$\mathrm{Aut}(H_q(m,n)) = T.((\mathrm{GL}_m(q) \circ \mathrm{GL}_n(q)).\,\mathrm{Aut}(\mathbb{F}_q)).$$

Theorem (H–Praeger 2025+)

Let C be a NT code in $H_q(m_1,m_2)$ with minimum distance $\delta \geq 3$, $O \in C$ and $G = \mathrm{Aut}(C)$. Then

1. $T \cap G \neq 1$ and C contains a non-trivial linear subcode.
2. G_O contains $H_1 \circ H_2$, where $s_1, s_2 \geq \delta$, $s_i \mid m_i$, and
    - $\mathrm{SL}_{m_i/s_i}(q^{s_i})$, $\mathrm{Sp}_{m_i/s_i}(q^{s_i})$ or $G_2(q^{s_i})' \leq H_i$.
3. C projects down to an $m_1/s_1 \times m_2/s_2$ block system of NT codes each with minimum distance δ in $H_q(s,t)$.

Examples exist in each case.

Open problems

Open questions:

- Can we classify all minimal linear NT codes?
- Find non-linear NT extensions of linear codes.

Thanks!

Thanks for your attention!