Stabilizers of graphs of linear functions and rank-metric codes

Valentino Smaldore

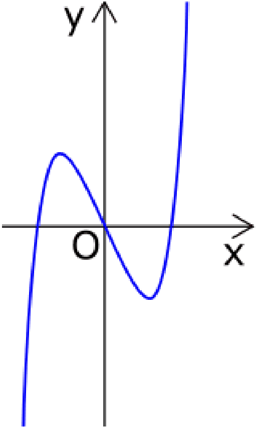
Università degli Studi di Padova

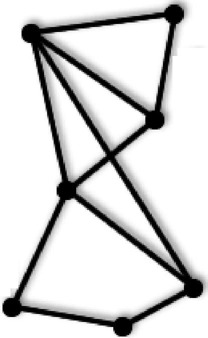
WCC 2024:The Thirteenth International Workshop on Coding and Cryptography

joint work with C. Zanella and F. Zullo

June 18, 2024

Graphs





Rank-metric codes

Definitions

Definition

An $\mathbb{F}_q$-linear rank-metric linear code $\mathcal{C}$ is a $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{m\times n}$ of $m \times n$ matrices over $\mathbb{F}_q$.

Definition

- *The rank distance between two matrices A and B is the rank of their difference: $d(A, B) = rk(A - B)$.*
- *The minimum distance of $\mathcal{C}$ is $d = d(\mathcal{C}) = min\{d(A, B) | A, B \in \mathcal{C}, A \neq B\}$.*

In this case we say $\mathcal{C}$ is a rank-metric code with parameters $(m, n, q; d)$.

Rank-metric codes

Definitions

Theorem (Singleton-like bound)

$$log_q|\mathcal{C}| \leq max\{m,n\}(min\{m,n\} - d + 1).$$

Definition

A code attaining the Singleton-like bound is called MRD-code.

Rank-metric codes

Left and right idealizers

Definition

The left and right idealizers of a rank-metric code $\mathcal{C}$ are

$$L(\mathcal{C}) = \{Y \in \mathbb{F}_q^{m\times m} \mid YC \in \mathcal{C}, \forall C \in \mathcal{C}\},$$

$$R(\mathcal{C}) = \{Z \in \mathbb{F}_q^{n\times n} \mid CZ \in \mathcal{C}, \forall C \in \mathcal{C}\}.$$

Theorem

1. *If $\mathcal{C}$ and $\mathcal{C}'$ are equivalent $\mathbb{F}_q$-linear rank-metric codes of $\mathbb{F}_q^{m\times n}$, then their left and right idealizers are isomorphic.*
2. *Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear MRD-code with $d > 1$.*
   - *If $m \leq n$, then $L(\mathcal{C})$ is a finite field with $|L(\mathcal{C})| \leq q^m$.*
   - *If $m \geq n$, then $R(\mathcal{C})$ is a finite field with $|R(\mathcal{C})| \leq q^n$.*
   - *If $m = n$, $L(\mathcal{C})$ and $R(\mathcal{C})$ are both finite fields.*

Rank-metric codes

Equivalent definitions

The elements of an $\mathbb{F}_q$-linear rank metric code $\mathcal{C}$ with parameters $(m, n, q; d)$ may be seen as:

- matrices of $\mathbb{F}_q^{m\times n}$ having rank at least d and with at least one matrix of rank exactly d;
- vectors of length n over $\mathbb{F}_{q^m}$ having norm rank at least d and with at least one vector of norm rank exactly d;
- $\mathbb{F}_q$-linear maps $V \to W$ where $V = V(n, q)$ and $W = V(m, q)$, having usual map rank at least d and with at least one map of rank exactly d;
- when $m = n$, elements of the $\mathbb{F}_q$-algebra $\mathcal{L}_{n,q}$ of q-polynomials over $\mathbb{F}_{q^n}$ modulo $x^{q^n} - x$, having rank at least d and with at least one polynomial of rank exactly d.

Linearized polynomials

$q = p^h$, $n \in \mathbb{N}$.

Definition

- *A linearized polynomial over* $\mathbb{F}_{q^n}$ *is*

$$f = \sum_{i=0}^{k} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$$

- *If* $a_k \neq 0$ *then the* q*-degree of* f *is* k.
- $L_{n,q}$ *will denote the set of linearized polynomials over* $\mathbb{F}_{q^n}$.
- $\mathcal{L}_{n,q} = L_{n,q}/(x^{q^n} - x)$.

Note that we can identify the elements of $\mathcal{L}_{n,q}$ with the q-polynomials having q-degree smaller than n.

Linearized polynomials

Partially scattered polynomials

Let t be a divisor of n, $1 < t < n$, f linearized polynomial over $\mathbb{F}_{q^n}$,

Definition

- *f is L-q^t-partially scattered if for any $y, z \in \mathbb{F}^*_{q^n}$,*

$$\frac{f(y)}{y} = \frac{f(z)}{z} \Longrightarrow \frac{y}{z} \in \mathbb{F}_{q^t}.$$

- *f is R-q^t-partially scattered if for any $y, z \in \mathbb{F}^*_{q^n}$,*

$$\frac{f(y)}{y} = \frac{f(z)}{z} \text{ and } \frac{y}{z} \in \mathbb{F}_{q^t} \Longrightarrow \frac{y}{z} \in \mathbb{F}_q.$$

Linearized polynomials

Scattered polynomials

Definition

A linearized polynomial f over $\mathbb{F}_{q^n}$ is scattered if for any $y, z \in \mathbb{F}^*_{q^n}$,

$$\frac{f(y)}{y} = \frac{f(z)}{z} \Longrightarrow \frac{y}{z} \in \mathbb{F}_q.$$

Note that a polynomial f which is both L-q^t-partially scattered and R-q^t-partially scattered is scattered.

Proposition (J. Sheekey, 2016)

Let f be a scattered polynomial over $\mathbb{F}_{q^n}$. Then $\mathcal{C}_f = \langle x, f(x) \rangle_{q^n}$ is a $(n, n, q; n-1)$-MRD code of dimension $2n$.

Linearized polynomials

Graph of functions

Definition

Let $f \in \mathbb{F}_q[x]$.

- *The graph of* f *is* $\mathcal{G}_f = \{(y, f(y)) \mid y \in \mathbb{F}_q\} \subseteq AG(2, q)$.
- *The set of directions of* $f \in \mathbb{F}_q[x]$ *is defined as*

$$\mathcal{D}_f = \{PQ \cap \ell_\infty \mid P, Q \in \mathcal{G}_f,\ \ P \neq Q\}.$$

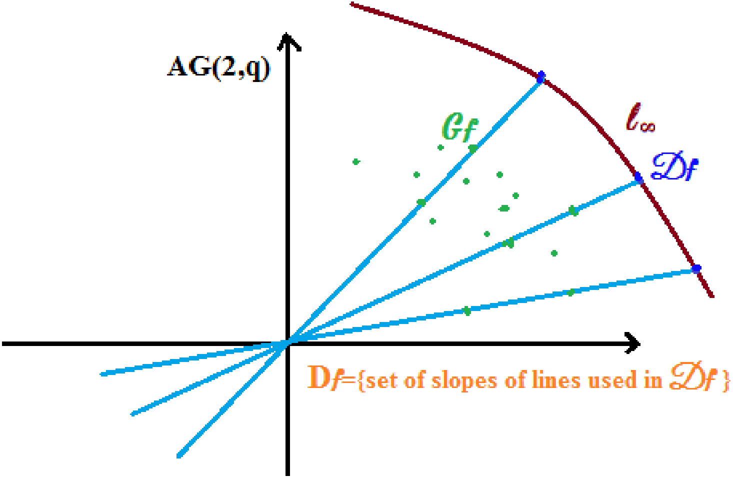
- *The set of slopes of the lines used in* $\mathcal{D}_f$ *is*

$$D_f = \left\{ \frac{f(y) - f(z)}{y - z} \mid y, z \in \mathbb{F}_q,\ \ y \neq z \right\}.$$

Note that $\mathcal{D}_f = \{\langle(1, m, 0)\rangle_q \mid m \in D_f\}$.

Linearized polynomials

Graph of functions



Linearized polynomials

Linear sets

Definition

- *The linear set associated to f is*

$$L_f = L_{\mathcal{G}_f} = \{\langle (y, f(y)) \rangle_{q^n} \mid y \in \mathbb{F}_{q^n}^*\}.$$

- *The weight of a point $P = \langle v \rangle_{q^n} \in PG(1, q^n)$ in L_f is*

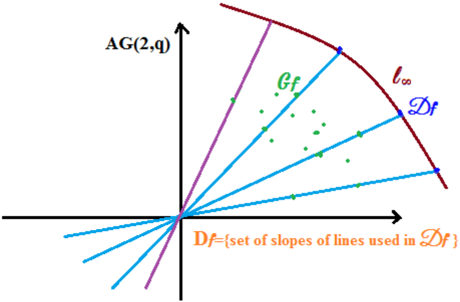
$$w_{L_f}(P) = \dim_q(\mathcal{G}_f \cap \langle v \rangle_{q^n}).$$

- *L_f is called scattered if all points of L_f have weight one.*

Note that the polynomial $f \in \mathcal{L}_{n,q}$ is scattered if and only if L_f is.

Linearized polynomials

Graph of functions



If ℓ meets $\mathcal{D}_f$ in a point of weight j, then it meets $\mathcal{G}_f$ in q^j points.
If ℓ meets ℓ_∞ outside $\mathcal{D}_f$, then it meets $\mathcal{G}_f$ in exactly 1 point.

Linearized polynomials

Low weight polynomials

Definition

A low weight polynomial f is a polynomial for which the associated linear set L_f has all points of weight less than $\frac{n}{2}$.

Example

Scattered polynomials have all points of weight 1, then they are low weight.

Stabilizers of graphs

Definition

The stabilizer of $\mathcal{G}_f$ *is the set* $\mathbb{S}_f = \{A \in \mathbb{F}_{q^n}^{2\times 2} \mid A\mathcal{G}_f \subseteq \mathcal{G}_f\}$, *where*

$$A\mathcal{G}_f = \left\{ A\begin{pmatrix} y \\ f(y) \end{pmatrix} \mid y \in \mathbb{F}_{q^n} \right\}.$$

Proposition

$\mathbb{S}_f$, *together with* $+$ *and* $\cdot$ *the usual sum and product of matrices in* $\mathbb{F}_{q^n}^{2\times 2}$ *and* $\star$ *the multiplication by a scalar in* $\mathbb{F}_q$, *forms an* $\mathbb{F}_q$*-algebra.*

Is $\mathbb{S}_f$ a field?

Stabilizers of graphs

Proposition

If $A, B \in \mathbb{S}_f$, then $A + B,\ AB \in \mathbb{S}_f$.

Theorem

If f is a low weight polynomial, then $(\mathbb{S}_f, +, \cdot)$ is a field.

Proof.

(Sketch of...) It is enough to prove that for any rank-one 2×2 matrix M with elements in $\mathbb{F}_{q^n}$, $M\mathcal{G}_f$ is not contained in $\mathcal{G}_f$. Consider $Z \neq O$ such that $MZ = O$ and let C be a nonzero column of M. Define $\mu : \mathcal{G}_f \to \mathbb{F}_{q^n}^2$, $(y, f(y)) \mapsto M(y, f(y))^T$. $\ker \mu \subseteq \langle Z \rangle_{q^n} \cap \mathcal{G}_f \Rightarrow dim_q(\ker \mu) < \frac{n}{2}$, then $\dim_q(Im\mu) > \frac{n}{2}$. Assume $M\mathcal{G}_f \subseteq \mathcal{G}_f$, then $Im\mu \subseteq \langle C \rangle_{q^n} \cap \mathcal{G}_f$, $\dim_q(Im\mu) < \frac{n}{2}$!! □

Stabilizers of graphs

Low weight polynomials and stabilizing fields

We will now see examples of low weight polynomials.

- $f = x^{q^s} \in \mathcal{L}_{n,q}$ with $(s,n)=1$, then $|\mathbb{S}_f| = q^n$;
- $f = \delta x^{q^s} + x^{q^{n(s-1)}} \in \mathcal{L}_{n,q}$ with $(s,n)=1$, $\delta \neq 0$ and $n \geq 4$, then $|\mathbb{S}_f| = q^2$ if n is even and $|\mathbb{S}_f| = q$ if n is odd;
- $f = \delta x^{q^s} + x^{q^{s+n/2}} \in \mathcal{L}_{n,q}$ with $\delta \neq 0$, n even and $(s,n)=1$, then $|\mathbb{S}_f| = q^{\frac{n}{2}}$;
- $f = x^q + x^{q^3} + \delta x^{q^5} \in \mathcal{L}_{6,q}$ with q odd and $\delta^2 + \delta = 1$, then $|\mathbb{S}_f| = q^2$;
- $f = x^{q^s} + x^{q^{s(t-1)}} + \eta^{1+q^s} x^{q^{s(t+1)}} + \eta^{1-q^{s(2t-1)}} x^{q^{s(2t-1)}} \in \mathcal{L}_{n,q}$ with q odd prime power, $t,s,n \in \mathbb{N}$ with $n = 2t$, $t \geq 5$, $(s,n)=1$ and $N_{q^n/q^t}(\eta) = -1$, then $|\mathbb{S}_f| = q^2$;
- $f = x^{q^{s(t-1)}} + x^{q^{s(2t-1)}} + m(x^{q^s} - x^{q^{s(t+1)}}) \in \mathcal{L}_{n,q}$ with q odd prime power, $t,s,n \in \mathbb{N}$ with $n=2t$, $t \geq 5$, $\gcd(s,n)=1$, $m \in \mathbb{F}_q^t$, then $|\mathbb{S}_f| = q^2$.

Stabilizers of graphs

Partially scattered cases

Partially scattered polynomials are *almost* low weight.

Proposition

1. *If f is a R-q^t-partially scattered polynomial in $\mathcal{L}_{n,q}$, then $w_{L_f}(P) \leq \frac{n}{2}$ for any point $P \in PG(1, q^n)$.*
2. *If f is a L-q^t-partially scattered polynomial in $\mathcal{L}_{n,q}$, then $w_{L_f}(P) \leq t$ for any point $P \in PG(1, q^n)$.*

Stabilizers of graphs

Partially scattered cases

Theorem

Let t be a proper divisor of n. Let $f \in \mathbb{F}_{q^n}[x]$ be an L-q^t-partially scattered polynomial in $\mathcal{L}_{n,q}$. Then $\mathbb{S}_f$ is not a field if and only if f is equivalent to $\ell^{q^t} - \ell$ for some $\ell \in \mathcal{L}_{t,q}$, and $n = 2t$.

Example

Let $p = \sum_{k=0}^{n-1} \left(\sum_{\ell=0}^{t-1} (u_\ell + u_\ell^{q^s} \xi) \lambda_\ell^{*\,q^k} \right) x^{q^k}$, where $\{u_0, \ldots, u_{t-1}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^t}$ and $(\lambda_0^*, \ldots, \lambda_{n-1}^*)$ is the dual basis of $(u_0 + \mu u_0^{q^s} \xi, \ldots, u_{t-1} + \mu u_{t-1}^{q^s} \xi, u_0 + u_0^{q^s} \xi, \ldots, u_{t-1} + u_{t-1}^{q^s} \xi)$. Then p is an R-q^t-partially scattered polynomial and the stabilizer of $\mathcal{G}_p$ is not a field.

Applications on rank-metric codes

Theorem

Let $f \in \mathcal{L}_{n,q}$ and denote by $\mathcal{C}_f = \langle x, f(x) \rangle_{q^n}$ the associated rank metric code in $\mathcal{L}_{n,q}$. Suppose that $f \notin \langle x \rangle_{q^n}$. Then the $\mathcal{F}_q$-algebras $\mathbb{S}_f$ and $R(\mathcal{C}_f)$ are isomorphic.

Proof.

(Sketch of...) The isomorphism is:

$$\psi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ax + bf(x).$$

□

Applications on rank-metric codes

Right idealizers of rank-metric codes

Theorem (T. H. Randrianarisoa, 2020)

Let $\mathcal{C}_f = \langle x, f(x) \rangle_{q^n}$. *Then,*

$$d(\mathcal{C}_f) = n - max\{dim_q(\mathcal{G}_f \cap \langle v \rangle_{q^n}) \mid P = \langle v \rangle_{q^n} \in PG(1, q^n)\}.$$

Corollary

Let f *be a linearized polynomial in* $\mathcal{L}_{n,q}$.
If $d(\mathcal{C}_f) > \frac{n}{2}$, *then* $R(\mathcal{C}_f)$ *is a field.*

Applications on rank-metric codes

MRD codes associated with partially scattered polynomials

Proposition

If $n = tt'$ and $f \in \mathcal{L}_{n,q}$ is an R-q^t-partially scattered polynomial then $\tilde{\mathcal{C}}_f = \{F_{|\mathbb{F}_{q^t}} \mid \mathbb{F}_{q^t} \to \mathbb{F}_{q^t} \mid F \in \mathcal{C}_f\}$ is an MRD $(n, t, q; t-1)$-code.

- $\mathcal{L}_{t,n,q} = \{g \in \mathcal{L}_{n,q} \mid g(\mathbb{F}_{q^t}) = \mathbb{F}_{q^t}\}$;
- $g \approx g'$ if and only if $g|_{\mathbb{F}_{q^t}} = g'|_{\mathbb{F}_{q^t}}$;
- $\tilde{\pi} : \mathcal{L}_{n,q} \longrightarrow \mathcal{L}_{n,q}/\approx$;
- $\Phi : \tilde{\pi}(g) \in \mathcal{L}_{t,n,q}/\approx \longrightarrow g_{|\mathbb{F}_{q^t}} \in \mathcal{L}_{t,q}$.

Proposition

Let $f \in \mathcal{L}_{n,q}$ with $f \notin \langle x \rangle_{q^n}$ and such that f is R-q^t-partially scattered. Then, $|R(\tilde{\mathcal{C}}_f)| \geq |\mathcal{L}_{t,n,q} \cap R(\mathcal{C}_f)|$.


MAY
THE FORCE
BE WITH YOU