On the weight distribution of linear sets

Geertrui Van de Voorde
(Joint work with John Sheekey)

University of Canterbury, New Zealand

Irsee, 10–16 September 2017

How it started

- Translation KM-arcs of type 4: equivalent to linear sets of rank n in $\mathrm{PG}(1, 2^n)$ with
  - 1 point of weight 2
  - all other points of weight 1

How it started

- Translation KM-arcs of type 4: equivalent to linear sets of rank n in $\mathrm{PG}(1, 2^n)$ with
  - 1 point of weight 2
  - all other points of weight 1
- They only exist for certain parameter values. But why?

How it started

- Translation KM-arcs of type 4: equivalent to linear sets of rank n in $\mathrm{PG}(1, 2^n)$ with
  - 1 point of weight 2
  - all other points of weight 1
- They only exist for certain parameter values. But why?
- Can we say something about the number of points of weight 2 in a linear set of rank n?

How it started

- Translation KM-arcs of type 4: equivalent to linear sets of rank n in $\mathrm{PG}(1, 2^n)$ with
  - 1 point of weight 2
  - all other points of weight 1
- They only exist for certain parameter values. But why?
- Can we say something about the number of points of weight 2 in a linear set of rank n?
- Can we deduce properties of the weight distribution of a linear set of rank n?

The plan

- Translate the problem to a problem about the rank distribution of a rank metric code $\mathcal{C}$.
- Give a geometrical translation of the problem.

The plan

- Translate the problem to a problem about the rank distribution of a rank metric code $\mathcal{C}$.
- Give a geometrical translation of the problem.
- Use MacWilliams identities to gather information about the rank distribution of the dual code $\mathcal{C}^{\perp}$
- Give a geometrical interpretation to the dualisation.

THE PLAN

- Translate the problem to a problem about the rank distribution of a rank metric code $\mathcal{C}$.
- Give a geometrical translation of the problem.
- Use MacWilliams identities to gather information about the rank distribution of the dual code $\mathcal{C}^{\perp}$
- Give a geometrical interpretation to the dualisation.

Linear sets of rank n in $\mathrm{PG}(1, q^n)$

'Definition'

A linear set of rank n in $\mathrm{PG}(1, q^n)$ is a set of the form

$$\{\langle (f(x), g(x)) \rangle_{\mathbb{F}_{q^n}} | x \in \mathbb{F}^*_{q^n}\},$$

where f and g are $\mathbb{F}_q$-linear maps from $\mathbb{F}_{q^n}$ to itself, and f and g have no (non-trivial) common kernel.

LINEAR SETS OF RANK n IN $\mathrm{PG}(1, q^n)$

'DEFINITION'

A linear set of rank n in $\mathrm{PG}(1, q^n)$ is a set of the form

$$\{\langle (f(x), g(x))\rangle_{\mathbb{F}_{q^n}} | x \in \mathbb{F}_{q^n}^*\},$$

where f and g are $\mathbb{F}_q$-linear maps from $\mathbb{F}_{q^n}$ to itself, and f and g have no (non-trivial) common kernel.

NOTE

If $x = \lambda a$, $\lambda \in \mathbb{F}_q^*$, then

$$\langle (f(x), g(x))\rangle_{\mathbb{F}_{q^n}} = \langle \lambda(f(a), \lambda g(a))\rangle_{\mathbb{F}_{q^n}} = \langle (f(a), g(a))\rangle_{\mathbb{F}_{q^n}}.$$

WEIGHTS OF LINEAR SETS OF RANK n IN $\mathrm{PG}(1, q^n)$

$$\langle (f(x), g(x)) \rangle_{\mathbb{F}_{q^n}} = \langle (f(a), g(a)) \rangle_{\mathbb{F}_{q^n}}$$

$$\Updownarrow$$

$$\begin{cases} f(x) = \mu f(a) \\ g(x) = \mu g(a) \end{cases} \quad \text{for some } \mu \in \mathbb{F}_{q^n}^*. \quad (*)$$

WEIGHTS OF LINEAR SETS OF RANK n IN $\mathrm{PG}(1, q^n)$

$$\langle (f(x), g(x)) \rangle_{\mathbb{F}_{q^n}} = \langle (f(a), g(a)) \rangle_{\mathbb{F}_{q^n}}$$

$$\Updownarrow$$

$$\begin{cases} f(x) = \mu f(a) \\ g(x) = \mu g(a) \end{cases} \quad \text{for some } \mu \in \mathbb{F}_{q^n}^*. \qquad (*)$$

DEFINITION

The dimension (over $\mathbb{F}_q$) of the solution space to $(*)$ is the weight of the point $\langle (f(a), g(a)) \rangle_{\mathbb{F}_{q^n}}$.

Note that

$$\begin{cases} f(x) = \mu f(a) \\ g(x) = \mu g(a) \end{cases} \quad \text{for some } \mu \in \mathbb{F}_{q^n}^*. \quad (*)$$

if and only if $g(a)f(x) - f(a)g(x) = (g(a)f - f(a)g)(x) = 0$.

Weights of linear sets of rank n in $\mathrm{PG}(1, q^n)$

Note that

$$\begin{cases} f(x) = \mu f(a) \\ g(x) = \mu g(a) \end{cases} \quad \text{for some } \mu \in \mathbb{F}^*_{q^n}. \quad (*)$$

if and only if $g(a)f(x) - f(a)g(x) = (g(a)f - f(a)g)(x) = 0$.

COROLLARY

Weight of $\langle (f(a), g(a)) \rangle_{\mathbb{F}_{q^n}}$ =dimension of kernel of $g(a)f - f(a)g$.

$$= n - rank(g(a)f - f(a)g)$$

Representing $\mathbb{F}_q$-linear maps

Linearised polynomials

If f is an $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^n}$, then

$$\begin{aligned} f : \mathbb{F}_{q^n} &\to \mathbb{F}_{q^n} \\ x &\mapsto f_0 x + f_1 x^q + f_2 x^{q^2} + \ldots + f_{n-1} x^{q^{n-1}} \end{aligned}$$

Representing $\mathbb{F}_q$-linear maps

Linearised polynomials

If f is an $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^n}$, then

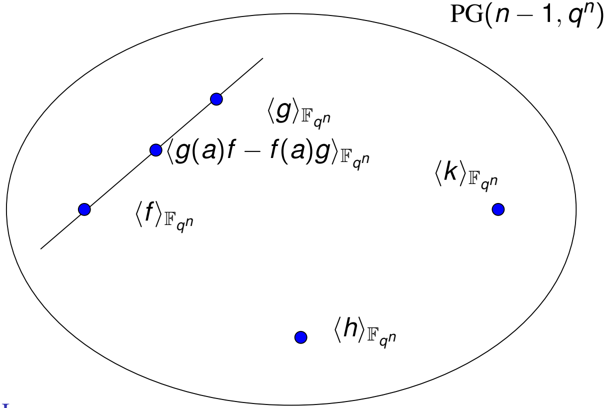
$$\begin{aligned} f : \mathbb{F}_{q^n} &\to \mathbb{F}_{q^n} \\ x &\mapsto f_0 x + f_1 x^q + f_2 x^{q^2} + \ldots + f_{n-1} x^{q^{n-1}} \end{aligned}$$

Correspondence

Every $\mathbb{F}_q$-linear map f, determines

$$\langle f \rangle_{\mathbb{F}_{q^n}} = \langle (f_0, \ldots, f_{n-1}) \rangle_{\mathbb{F}_{q^n}}$$

a point in $\mathrm{PG}(n-1, q^n)$.



RECALL

Weight of $\langle (f(a), g(a)) \rangle_{\mathbb{F}_{q^n}} = n - rank(g(a)f - f(a)g)$

Correspondence

Definition

Point $\langle f \rangle_{\mathbb{F}_{q^n}}$ has rank k if and only if f has rank k.

Maps of rank 1

Rank 1 linearized polynomial: of the form $x \mapsto \alpha \mathrm{Tr}(\beta x)$

Correspondence

Definition

Point $\langle f \rangle_{\mathbb{F}_{q^n}}$ has rank k if and only if f has rank k.

Maps of rank 1

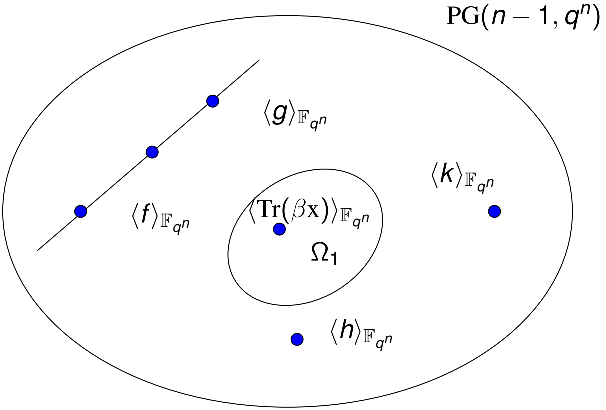
Rank 1 linearized polynomial: of the form $x \mapsto \alpha \mathrm{Tr}(\beta x)$

Ω_1: set of rank 1 points

$$\langle \alpha(\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{n-1}}) \rangle_{\mathbb{F}_{q^n}}.$$

Ω_1 is a subgeometry of $\mathrm{PG}(n-1, q^n)$.

CORRESPONDENCE



Correspondence

Maps of rank k

Rank k map: sum of k rank 1 maps

Correspondence

Maps of rank k

Rank k map: sum of k rank 1 maps

Secant varieties

Ω_2: set of all point that lie on an extended line of the subgeometry Ω_1

Ω_k: set of rank k points

Putting it all together

- $L_{f,g} = \{\langle f(x), g(x)\rangle_{\mathbb{F}_{q^n}} | x \in \mathbb{F}^*_{q^n}\}$ is a scattered linear set of rank n if and only if the line $\langle f, g\rangle_{\mathbb{F}_{q^n}}$ in $\mathrm{PG}(n-1, q^n)$ is skew from Ω_{n-2}.
- $L_{f,g}$ has one point of weight 2 and all others of weight one if the line $\langle f, g\rangle_{\mathbb{F}_{q^n}}$ in $\mathrm{PG}(n-1, q^n)$ is a tangent line to Ω_{n-2}.

Putting it all together

- $L_{f,g} = \{\langle f(x), g(x)\rangle_{\mathbb{F}_{q^n}} | x \in \mathbb{F}^*_{q^n}\}$ is a scattered linear set of rank n if and only if the line $\langle f, g\rangle_{\mathbb{F}_{q^n}}$ in $\mathrm{PG}(n-1, q^n)$ is skew from Ω_{n-2}.
- $L_{f,g}$ has one point of weight 2 and all others of weight one if the line $\langle f, g\rangle_{\mathbb{F}_{q^n}}$ in $\mathrm{PG}(n-1, q^n)$ is a tangent line to Ω_{n-2}.
- weight distribution of $L_{f,g}$ $\leftrightarrow$ intersection of $\langle f, g\rangle_{\mathbb{F}_{q^n}}$ with $\Omega'_k s$.

Putting it all together

- $L_{f,g} = \{\langle f(x), g(x)\rangle_{\mathbb{F}_{q^n}} | x \in \mathbb{F}^*_{q^n}\}$ is a scattered linear set of rank n if and only if the line $\langle f, g\rangle_{\mathbb{F}_{q^n}}$ in $\mathrm{PG}(n-1, q^n)$ is skew from Ω_{n-2}.
- $L_{f,g}$ has one point of weight 2 and all others of weight one if the line $\langle f, g\rangle_{\mathbb{F}_{q^n}}$ in $\mathrm{PG}(n-1, q^n)$ is a tangent line to Ω_{n-2}.
- weight distribution of $L_{f,g} \leftrightarrow$ intersection of $\langle f, g\rangle_{\mathbb{F}_{q^n}}$ with $\Omega'_k s$.

Downside

Hard to deduce geometrical information about intersection with Ω_k's

Rank-metric codes

- Codewords: $\mathbb{F}_q$-linear maps

RANK-METRIC CODES

- Codewords: $\mathbb{F}_q$-linear maps
- If you prefer matrices:

$$A_f = \begin{pmatrix} f_0 & f_1 & & \cdots & f_{n-2} & f_{n-1} \\ f_{n-1}^q & f_0^q & & \cdots & f_{n-3}^q & f_{n-2}^q \\ f_{n-2}^{q^2} & f_{n-1}^{q^2} & f_0^{q^2} & \cdots & f_{n-4}^{q^2} & f_{n-3}^{q^2} \\ \vdots & & & & & \vdots \\ f_1^{q^{n-1}} & f_2^{q^{n-1}} & & \cdots & f_{n-1}^{q^{n-1}} & f_0^{q^{n-1}} \end{pmatrix}$$

- Rank of f=rank of A_f.
- Points on $\langle f, g \rangle_{\mathbb{F}_{q^n}} \leftrightarrow \mathbb{F}_{q^n}$-linear combinations of f and g $\leftrightarrow$ $2n$-dimensional code $\mathcal{C}$ over $\mathbb{F}_q$.

Duality for rank-metric codes

$\mathcal{C} = \langle f, g \rangle$

Duality for rank-metric codes

$\mathcal{C} = \langle f, g \rangle$
$\mathcal{C}^{\perp} = \{h \mid f.h = g.h = 0\}$.

Duality for rank-metric codes

$\mathcal{C} = \langle f, g \rangle$
$\mathcal{C}^{\perp} = \{h \mid f.h = g.h = 0\}$.
$f.g = (f_0, \ldots, f_{n-1})(g_0, \ldots, g_{n-1}) = f_0 g_0 + f_1 g_1 + \ldots + f_{n-1} g_{n-1}$

Duality for rank-metric codes

$\mathcal{C} = \langle f, g \rangle$
$\mathcal{C}^\perp = \{h \mid f.h = g.h = 0\}$.

$f.g = (f_0, \ldots, f_{n-1})(g_0, \ldots, g_{n-1}) = f_0 g_0 + f_1 g_1 + \ldots + f_{n-1} g_{n-1}$

MacWilliams identities –Delsarte-Ravagnani

The rank distribution of $\mathcal{C}$ determines the rank distribution of $\mathcal{C}^\perp$.

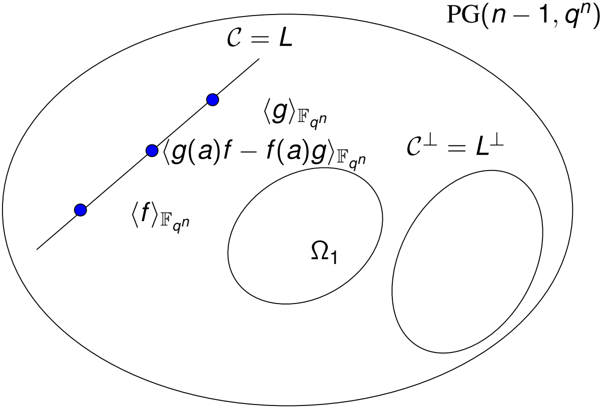
MacWilliams identities –Delsarte-Ravagnani

Theorem

If (A_i)*: rank distribution of* $\mathcal{C}$, $\mathcal{C} \subseteq M_{k\times m}(\mathbb{F}_q)$*, and* (B_i)*: rank distribution of* $\mathcal{C}^\perp$*, then for all* $0 \le \nu \le k$,

$$\sum_{i=0}^{k-\nu} A_i \begin{bmatrix} k-i \\ \nu \end{bmatrix} = \frac{|\mathcal{C}|}{q^{m\nu}} \sum_{j=0}^{\nu} B_j \begin{bmatrix} k-j \\ \nu - j \end{bmatrix}$$

BACK TO THE PICTURE (PROJECTIVE VERSION)



$\mathcal{C}$ and $\mathcal{C}^\perp$ are not necessarily skew

Back to the picture

Linear sets as projected subgeometries

$\Omega_1/L^\perp$ defines a linear set.

Back to the picture

Linear sets as projected subgeometries

$\Omega_1/L^\perp$ defines a linear set.

Theorem (Sheekey-VdV)

The linear set $\{\langle (f(x), g(x))\rangle_{\mathbb{F}_{q^n}} | x \in \mathbb{F}^*_{q^n}\}$ *is isomorphic to*

$$\Omega_1/\langle f, g\rangle^\perp_{\mathbb{F}_{q^n}}.$$

COROLLARY

weight distribution of $L_{f,g} = \{\langle (f(x), g(x)\rangle_{\mathbb{F}_{q^n}} | x \in \mathbb{F}_{q^n}^*\}$
$\leftrightarrow$ *rank distribution of* $\langle f, g\rangle_{\mathbb{F}_{q^n}}$
$\leftrightarrow$ *rank distribution of* $\langle f, g\rangle_{\mathbb{F}_{q^n}}^{\perp}$ *(MacWilliams)*

COROLLARY

weight distribution of $L_{f,g} = \{\langle (f(x), g(x)\rangle_{\mathbb{F}_{q^n}} | x \in \mathbb{F}^*_{q^n}\}$
$\leftrightarrow$ *rank distribution of* $\langle f, g\rangle_{\mathbb{F}_{q^n}}$
$\leftrightarrow$ *rank distribution of* $\langle f, g\rangle^{\perp}_{\mathbb{F}_{q^n}}$ *(MacWilliams)*
$\leftrightarrow$ *weight distribution of the linear set* $\{\langle (h_1(x), \ldots, h_{n-2}(x)\rangle_{\mathbb{F}_{q^n}} | x \in \mathbb{F}^*_{q^n}\}$*, where* $\langle h_i\rangle_{\mathbb{F}_{q^n}}$ *spans* $\langle f, g\rangle^{\perp}_{\mathbb{F}_{q^n}}$*.*

If $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are skew, this corresponds to switching the role of the spaces $\mathcal{C}$ and $\mathcal{C}^{\perp}$.

Points of weight 2 in a linear set on a projective line

- Take $\mathcal{L} = \{\langle (f(x), g(x)) \rangle_{\mathbb{F}_{q^n}} | x \in \mathbb{F}_{q^n}^*\}$ with only points of weight 1 and 2
- $\rightarrow$ line $L = \langle f, g \rangle_{\mathbb{F}_{q^n}}$ in $\mathrm{PG}(n-1, q^n)$ with only points of ranks $n-2, n-1, n$
- $\rightarrow$ $n-3$ space $L^\perp$ with prescribed ranks
- $\rightarrow$ linear set Ω_1 / L with prescribed weights.

Points of weight 2 in a linear set on a projective line

- Take $\mathcal{L} = \{\langle (f(x), g(x)) \rangle_{\mathbb{F}_{q^n}} | x \in \mathbb{F}_{q^n}^*\}$ with only points of weight 1 and 2
- $\rightarrow$ line $L = \langle f, g \rangle_{\mathbb{F}_{q^n}}$ in $\mathrm{PG}(n-1, q^n)$ with only points of ranks $n-2, n-1, n$
- $\rightarrow$ $n-3$ space $L^{\perp}$ with prescribed ranks
- $\rightarrow$ linear set Ω_1 / L with prescribed weights.

Our hope

Find a contradiction for some parameter sets.

Points of weight 2 in a linear set on a projective line

- Take $\mathcal{L} = \{\langle (f(x), g(x)) \rangle_{\mathbb{F}_{q^n}} | x \in \mathbb{F}_{q^n}^*\}$ with only points of weight 1 and 2
- $\rightarrow$ line $L = \langle f, g \rangle_{\mathbb{F}_{q^n}}$ in $\mathrm{PG}(n-1, q^n)$ with only points of ranks $n-2, n-1, n$
- $\rightarrow$ $n-3$ space $L^{\perp}$ with prescribed ranks
- $\rightarrow$ linear set Ω_1/L with prescribed weights.

Our hope

Find a contradiction for some parameter sets. Doesn't work unfortunately!

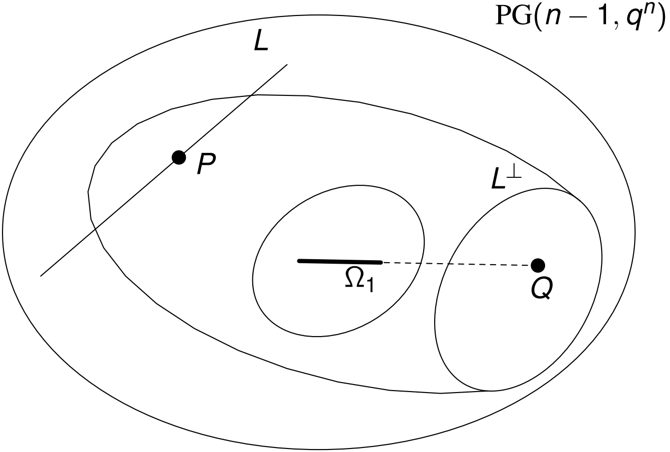
One of the MacWilliams identities

$$B_2 = \sum_{i=1}^{n-2} A_i \left[\begin{array}{c} n-i-1 \\ 1 \end{array} \right]$$

Corollary

If there are only points of weight 1 *and* 2 *in a linear set* $\Omega_1/L^\perp$*, then* $B_2 = A_{n-2}$*, i.e. the number of points of weight* 2 *in* $\Omega_1/L^\perp$ *is the number of points of rank* 2 *in* $L^\perp$*.*

Geometric point of view




To be continued...

Thank you for your attention!