Linear sets in the projective line over the endomorphism ring of a finite field

Hans Havlicek and Corrado Zanella

TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

Research Group
Differential Geometry and Geometric Structures
Institute of Discrete Mathematics and Geometry

UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Tecnica e Gestione
dei Sistemi Industriali

Finite Geometries – Fifth Irsee Conference,
September 11, 2017

Basic assumptions

- Let q be a prime power and let $t \geq 2$ be an integer.

Basic assumptions

- Let q be a prime power and let $t \geq 2$ be an integer.
- The field with q^t elements is denoted by $\mathbb{F}_{q^t}$ and its unique subfield of order q is written as $\mathbb{F}_q$.

Basic assumptions

- Let q be a prime power and let $t \geq 2$ be an integer.
- The field with q^t elements is denoted by $\mathbb{F}_{q^t}$ and its unique subfield of order q is written as $\mathbb{F}_q$.
- The vector space $\mathbb{F}_{q^t}^2$ over $\mathbb{F}_{q^t}$ determines the projective line $\mathrm{PG}(1, q^t)$. Its points have the form

$$\langle (u, v) \rangle_{q^t} \text{ with } (0, 0) \neq (u, v) \in \mathbb{F}_{q^t}^2.$$

Basic assumptions

- Let q be a prime power and let $t \geq 2$ be an integer.
- The field with q^t elements is denoted by $\mathbb{F}_{q^t}$ and its unique subfield of order q is written as $\mathbb{F}_q$.
- The vector space $\mathbb{F}_{q^t}^2$ over $\mathbb{F}_{q^t}$ determines the projective line $\mathrm{PG}(1, q^t)$. Its points have the form

$$\langle (u, v) \rangle_{q^t} \ \text{ with } \ (0, 0) \neq (u, v) \in \mathbb{F}_{q^t}^2.$$

- The vector space $\mathbb{F}_{q^t}^2$ over $\mathbb{F}_q$ determines the projective space $\mathrm{PG}(2t - 1, q)$. Its points have the form

$$\langle (u, v) \rangle_{q} \ \text{ with } \ (0, 0) \neq (u, v) \in \mathbb{F}_{q^t}^2.$$

Basic assumptions

- Let q be a prime power and let $t \geq 2$ be an integer.
- The field with q^t elements is denoted by $\mathbb{F}_{q^t}$ and its unique subfield of order q is written as $\mathbb{F}_q$.
- The vector space $\mathbb{F}_{q^t}^2$ over $\mathbb{F}_{q^t}$ determines the projective line $\mathrm{PG}(1, q^t)$. Its points have the form

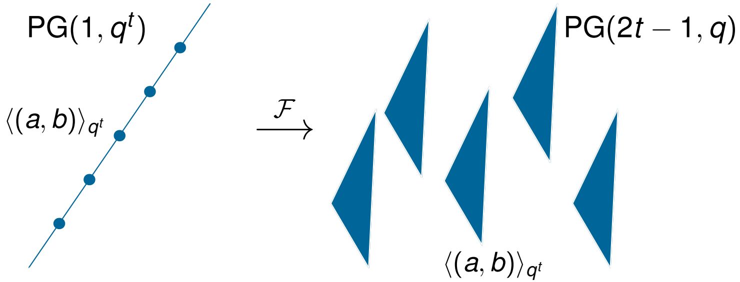
$$\langle (u, v) \rangle_{q^t} \ \text{ with } \ (0,0) \neq (u, v) \in \mathbb{F}_{q^t}^2.$$

- The vector space $\mathbb{F}_{q^t}^2$ over $\mathbb{F}_q$ determines the projective space $\mathrm{PG}(2t-1, q)$. Its points have the form

$$\langle (u, v) \rangle_{q} \ \text{ with } \ (0,0) \neq (u, v) \in \mathbb{F}_{q^t}^2.$$

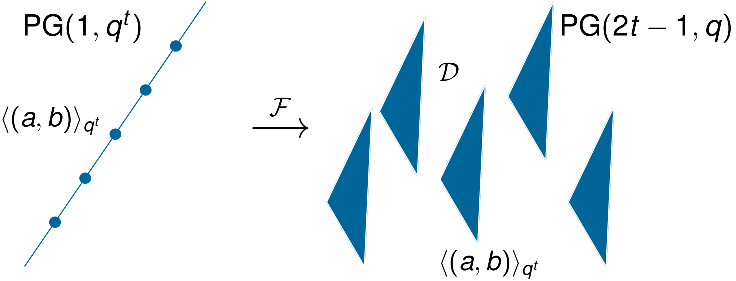
- $\mathcal{G}$ denotes the Grassmannian of $(t-1)$-dimensional subspaces of $\mathrm{PG}(2t-1, q)$.

Field reduction map $\mathcal{F}$: $\mathrm{PG}(1, q^t) \to \mathcal{G}$



The *field reduction map* $\mathcal{F}$ assigns to each point $\langle (a, b) \rangle_{q^t}$ that element of the Grassmannian $\mathcal{G}$ which is given by $\langle (a, b) \rangle_{q^t}$ (considered as subspace of the vector space $\mathbb{F}_{q^t}^2$ over $\mathbb{F}_q$).

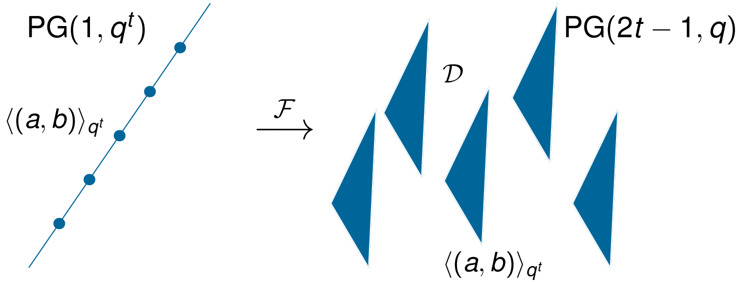
Field reduction map $\mathcal{F}$: $\mathrm{PG}(1, q^t) \to \mathcal{G}$



The *field reduction map* $\mathcal{F}$ assigns to each point $\langle (a,b) \rangle_{q^t}$ that element of the Grassmannian $\mathcal{G}$ which is given by $\langle (a,b) \rangle_{q^t}$ (considered as subspace of the vector space $\mathbb{F}_{q^t}^2$ over $\mathbb{F}_q$).

The image of $\mathcal{F}$ is a Desarguesian spread, say $\mathcal{D}$.

Field reduction map $\mathcal{F}$: $\mathrm{PG}(1, q^t) \to \mathcal{G}$

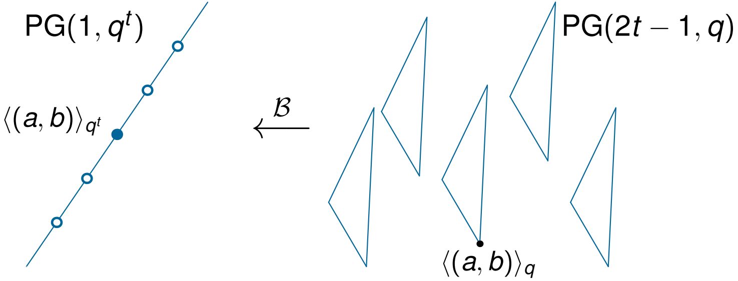


The *field reduction map* $\mathcal{F}$ assigns to each point $\langle(a, b)\rangle_{q^t}$ that element of the Grassmannian $\mathcal{G}$ which is given by $\langle(a, b)\rangle_{q^t}$ (considered as subspace of the vector space $\mathbb{F}_{q^t}^2$ over $\mathbb{F}_q$).

The image of $\mathcal{F}$ is a Desarguesian spread, say $\mathcal{D}$.

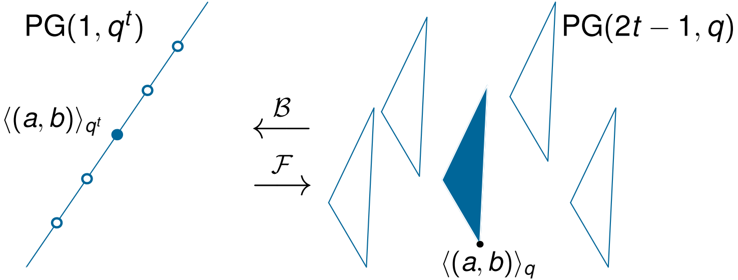
The map $\mathcal{F}$ is injective.

Blow up map $\mathcal{B}$: PG$(2t-1, q) \to$ PG$(1, q^t)$



The *blow up map* $\mathcal{B}$ assigns to each point $\langle (a, b)\rangle_q$ the point $\langle (a, b)\rangle_{q^t}$.

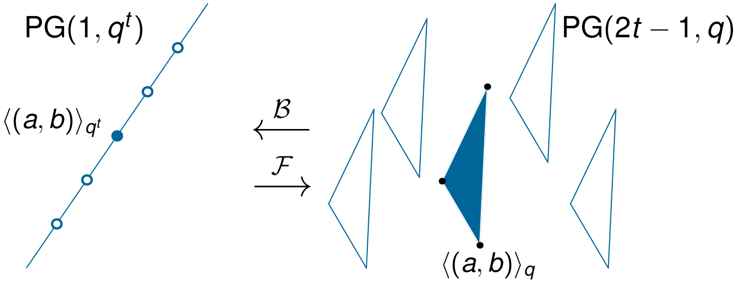
Blow up map $\mathcal{B}$: $\mathrm{PG}(2t-1,q) \to \mathrm{PG}(1,q^t)$



The *blow up map* $\mathcal{B}$ assigns to each point $\langle (a,b)\rangle_q$ the point $\langle (a,b)\rangle_{q^t}$.

The product $\mathcal{BF}$: $\mathrm{PG}(2t-1,q) \to \mathcal{G}$ takes $\langle (a,b)\rangle_q$ to the only element of the spread $\mathcal{D}$ containing $\langle (a,b)\rangle_q$.

Blow up map $\mathcal{B}\colon \mathrm{PG}(2t-1,q) \to \mathrm{PG}(1,q^t)$

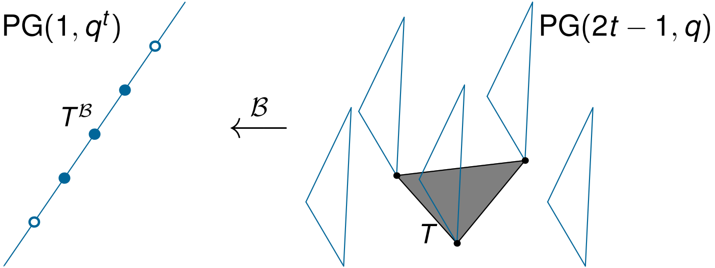


The *blow up map* $\mathcal{B}$ assigns to each point $\langle(a,b)\rangle_q$ the point $\langle(a,b)\rangle_{q^t}$.

The product $\mathcal{BF}\colon \mathrm{PG}(2t-1,q) \to \mathcal{G}$ takes $\langle(a,b)\rangle_q$ to the only element of the spread $\mathcal{D}$ containing $\langle(a,b)\rangle_q$.

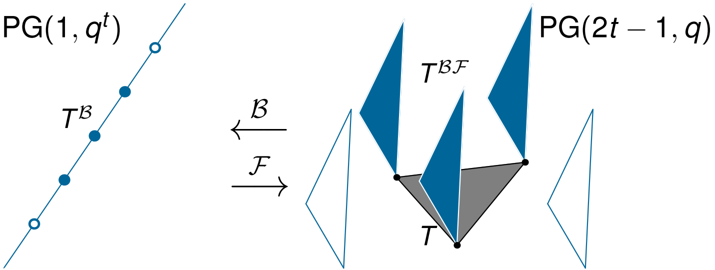
The map $\mathcal{B}$ is not injective (due to $t \geq 2$).

Linear sets



By blowing up all points of an element $T \in \mathcal{G}$ we obtain a subset $T^{\mathcal{B}}$ of PG$(1, q^t)$, which is called an $\mathbb{F}_q$-linear set of rank t.

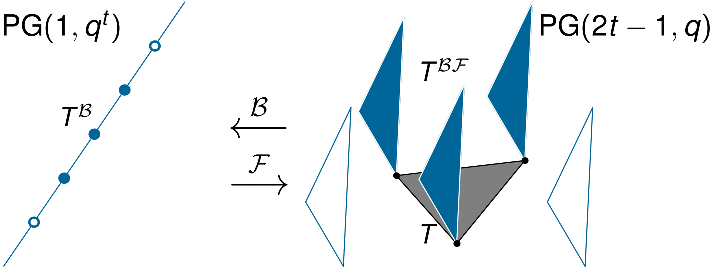
Linear sets



By blowing up all points of an element $T \in \mathcal{G}$ we obtain a subset $T^{\mathcal{B}}$ of $\mathrm{PG}(1, q^t)$, which is called an $\mathbb{F}_q$-linear set of rank t.

The set $T^{\mathcal{B}\mathcal{F}}$ comprises those elements of the spread $\mathcal{D}$ which intersect T non-trivially.

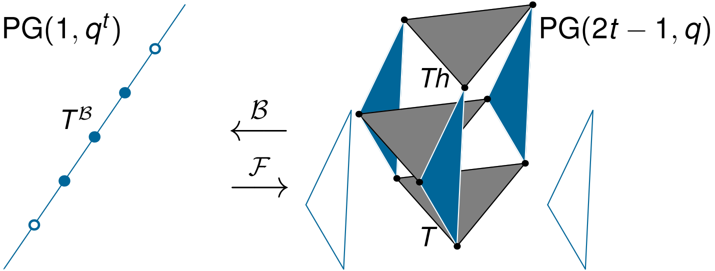
Linear sets



By blowing up all points of an element $T \in \mathcal{G}$ we obtain a subset $T^{\mathcal{B}}$ of $\mathrm{PG}(1, q^t)$, which is called an $\mathbb{F}_q$-linear set of rank t.

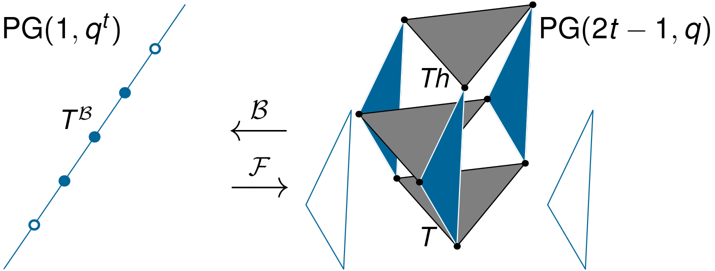
The set $T^{\mathcal{B}\mathcal{F}}$ comprises those elements of the spread $\mathcal{D}$ which intersect T non-trivially.
An element $T \in \mathcal{G}$ and its corresponding linear set $T^{\mathcal{B}}$ are said to be scattered if the restriction of $\mathcal{B}$ to T is injective.

Scattered linear sets – Two families



Let T be scattered and write $Th := \{\langle(ah, bh)\rangle_q \mid \langle(a, b)\rangle_q \in T\}$, where $h \in \mathbb{F}_{q^t} \setminus \{0\} =: \mathbb{F}^*_{q^t}$.

Scattered linear sets – Two families



Let T be scattered and write $Th := \{\langle(ah, bh)\rangle_q \mid \langle(a, b)\rangle_q \in T\}$, where $h \in \mathbb{F}_{q^t} \setminus \{0\} =: \mathbb{F}^*_{q^t}$. Then the families

$$\mathcal{U}(T) := T^{\mathcal{B}\mathcal{F}} \text{ and } \mathcal{U}'(T) := \{Th \mid h \in \mathbb{F}^*_{q^t}\},$$

constitute two partitions (by elements of $\mathcal{G}$) of the same hypersurface of degree t in PG$(2t - 1, q)$.

See M. Lavrauw, J. Sheekey, C. Zanella [15, Prop. 2].

The projective line over E

- We consider the endomorphism ring

$$E := \mathrm{End}_q(\mathbb{F}_{q^t}).$$

The projective line over E

- We consider the endomorphism ring

$$E := \mathrm{End}_q(\mathbb{F}_{q^t}).$$

- An element $(\alpha, \beta) \in E^2$ is called *admissible* if it can be extended to a basis of the left E-module E^2.

The projective line over E

- We consider the endomorphism ring

$$E := \mathrm{End}_q(\mathbb{F}_{q^t}).$$

- An element $(\alpha, \beta) \in E^2$ is called *admissible* if it can be extended to a basis of the left E-module E^2.
- The *projective line over E* is the set $\mathrm{PG}(1, E)$ of all cyclic submodules $E(\alpha, \beta)$ of E^2, where $(\alpha, \beta) \in E^2$ is admissible. The elements of $\mathrm{PG}(1, E)$ are called *points*.

The projective line over E

- We consider the endomorphism ring

$$E := \mathrm{End}_q(\mathbb{F}_{q^t}).$$

- An element $(\alpha, \beta) \in E^2$ is called *admissible* if it can be extended to a basis of the left E-module E^2.
- The *projective line over E* is the set $\mathrm{PG}(1, E)$ of all cyclic submodules $E(\alpha, \beta)$ of E^2, where $(\alpha, \beta) \in E^2$ is admissible. The elements of $\mathrm{PG}(1, E)$ are called *points*.
- The map

$$\Psi : \mathrm{PG}(1, E) \to \mathcal{G} : E(\alpha, \beta) \mapsto \left\{ \langle (u^\alpha, u^\beta) \rangle_q \mid u \in \mathbb{F}^*_{q^t} \right\}$$

is a bijection (X. Hubaut [11], Z.-X. Wan [24], and others).

The distant relation

Let $P = E(\alpha, \beta)$ and $Q = E(\gamma, \delta)$ be points of $\mathrm{PG}(1, E)$.

The distant relation

Let $P = E(\alpha, \beta)$ and $Q = E(\gamma, \delta)$ be points of $\mathrm{PG}(1, E)$.

- P and Q are called *distant*, in symbols $P \vartriangle Q$, if $((\alpha, \beta), (\gamma, \delta))$ is a basis of E^2.

The distant relation

Let $P = E(\alpha, \beta)$ and $Q = E(\gamma, \delta)$ be points of $\mathrm{PG}(1, E)$.

- P and Q are called *distant*, in symbols $P \bigtriangleup Q$, if $((\alpha, \beta), (\gamma, \delta))$ is a basis of E^2.
- $P \bigtriangleup Q$ if, and only if, the subspaces P^Ψ and Q^Ψ are skew (see, among others, A. Blunck [1, Thm. 2.4]).

Embedding of $PG(1, q^t)$ in $PG(1, E)$

- The mapping

$$\mathbb{F}_{q^t} \to E\colon a \mapsto (\rho_a\colon x \mapsto xa)$$

is a monomorphism of rings taking $1 \in \mathbb{F}_{q^t}$ to the identity $\mathbb{1} \in E$.

Embedding of $\mathrm{PG}(1, q^t)$ in $\mathrm{PG}(1, E)$

- The mapping

$$\mathbb{F}_{q^t} \to E\colon a \mapsto (\rho_a\colon x \mapsto xa)$$

  is a monomorphism of rings taking $1 \in \mathbb{F}_{q^t}$ to the identity $\mathbb{1} \in E$.

- This allows us to define an embedding

$$\iota : \mathrm{PG}(1, q^t) \to \mathrm{PG}(1, E) : \langle (a, b) \rangle_{q^t} \mapsto E(\rho_a, \rho_b).$$

Projectivities

- Given a matrix
$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathsf{GL}_2(E)$$
we obtain a projectivity of $\mathsf{PG}(1, E)$ by letting
$$E(\xi, \eta) \mapsto E\left((\xi, \eta) \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right)$$
and a projectivity of $\mathsf{PG}(2t-1, q)$ by letting
$$\langle (u, v) \rangle_q \mapsto \langle (u^\alpha + v^\gamma, u^\beta + v^\delta) \rangle_q.$$

Projectivities

- Given a matrix
$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(E)$$
we obtain a projectivity of $\mathrm{PG}(1, E)$ by letting
$$E(\xi, \eta) \mapsto E\left((\xi, \eta) \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right)$$
and a projectivity of $\mathrm{PG}(2t - 1, q)$ by letting
$$\langle (u, v) \rangle_q \mapsto \langle (u^\alpha + v^\gamma, u^\beta + v^\delta) \rangle_q.$$
- All projectivities of $\mathrm{PG}(1, E)$ and $\mathrm{PG}(2t - 1, q)$ can be obtained in this way (S. Lang [13, 642–643]).

Projectivities

- Given a matrix

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(E)$$

we obtain a projectivity of $\mathrm{PG}(1, E)$ by letting

$$E(\xi, \eta) \mapsto E\left((\xi, \eta) \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right)$$

and a projectivity of $\mathrm{PG}(2t-1, q)$ by letting

$$\langle (u, v) \rangle_q \mapsto \langle (u^\alpha + v^\gamma, u^\beta + v^\delta) \rangle_q.$$

- All projectivities of $\mathrm{PG}(1, E)$ and $\mathrm{PG}(2t-1, q)$ can be obtained in this way (S. Lang [13, 642–643]).
- The actions of $\mathrm{GL}_2(E)$ on $\mathrm{PG}(1, E)$ and $\mathcal{G}$ are isomorphic.

Dictionary

$\mathrm{PG}(1, E)$	Grassmannian $\mathcal{G}$
point T	subspace $T^{\Psi} \in \mathcal{G}$
subline $\mathrm{PG}(1, q^t)^{\iota}$	spread $\mathcal{D}$
$L_T := \left\{ X \in \mathrm{PG}(1, q^t)^{\iota} \mid X \not\triangle T \right\}$	$\mathcal{U}(T^{\Psi}) = (T^{\Psi})^{\mathcal{BF}}$
$L'_T = \left\{ T \cdot \mathrm{diag}(\rho_h, \rho_h) \mid h \in \mathbb{F}^*_{q^t} \right\}$	$\mathcal{U}'(T^{\Psi})$

Dictionary

$\mathrm{PG}(1, E)$	Grassmannian $\mathcal{G}$
point T	subspace $T^{\Psi} \in \mathcal{G}$
subline $\mathrm{PG}(1, q^t)^{\iota}$	spread $\mathcal{D}$
$L_T := \left\{ X \in \mathrm{PG}(1, q^t)^{\iota} \mid X \not\triangle T \right\}$	$\mathcal{U}(T^{\Psi}) = (T^{\Psi})^{\mathcal{BF}}$
$L'_T = \left\{ T \cdot \mathrm{diag}(\rho_h, \rho_h) \mid h \in \mathbb{F}^*_{q^t} \right\}$	$\mathcal{U}'(T^{\Psi})$

The sets L_T, with T varying in $\mathrm{PG}(1, E)$, are precisely the images under ι of the $\mathbb{F}_q$-linear sets of rank t in $\mathrm{PG}(1, q^t)$.

Linear sets of pseudoregulus type

Let τ be a generator of the Galois group $\mathrm{Gal}(\mathbb{F}_{q^t}/\mathbb{F}_q)$ and write $T_0 := E(\mathbb{1}, \tau)$. Then L_{T_0} corresponds to a scattered linear set.

Linear sets of pseudoregulus type

Let τ be a generator of the Galois group $\mathrm{Gal}(\mathbb{F}_{q^t}/\mathbb{F}_q)$ and write $T_0 := E(\mathbb{1}, \tau)$. Then L_{T_0} corresponds to a scattered linear set.

A linear set of $\mathrm{PG}(1, q^t)$ is said to be of *pseudoregulus type* if it is projectively equivalent to the linear set corresponding to T_0.

Linear sets of pseudoregulus type

Let τ be a generator of the Galois group $\mathrm{Gal}(\mathbb{F}_{q^t}/\mathbb{F}_q)$ and write $T_0 := E(\mathbb{1}, \tau)$. Then L_{T_0} corresponds to a scattered linear set.

A linear set of $\mathrm{PG}(1, q^t)$ is said to be of *pseudoregulus type* if it is projectively equivalent to the linear set corresponding to T_0.

Cf. B. Czajbók, C. Zanella [4],
G. Donati, N. Durante [6],
M. Lavrauw, J. Sheekey, C. Zanella [15],
G. Lunardon, G. Marino, O. Polverino, R. Trombetti [20].

Main result

Theorem (H. H., C. Zanella [9])

A scattered linear set of $\mathrm{PG}(1, q^t)$, $t \geq 3$, *arising from* $T \in \mathrm{PG}(1, E)$ *is of pseudoregulus type if, and only if, there exists a projectivity* φ *of* $\mathrm{PG}(1, E)$ *such that* $L_T^{\varphi} = L'_T$.

Main result

Theorem (H. H., C. Zanella [9])

A scattered linear set of $\mathrm{PG}(1, q^t)$, $t \geq 3$, *arising from* $T \in \mathrm{PG}(1, E)$ *is of pseudoregulus type if, and only if, there exists a projectivity* φ *of* $\mathrm{PG}(1, E)$ *such that* $L_T^{\varphi} = L'_T$.

Proof.

"$\Leftarrow$" See M. Lavrauw, J. Sheekey, C. Zanella [15, Cor. 18] or [9].

Main result

Theorem (H. H., C. Zanella [9])

A scattered linear set of $\mathrm{PG}(1, q^t)$*,* $t \geq 3$*, arising from* $T \in \mathrm{PG}(1, E)$ *is of pseudoregulus type if, and only if, there exists a projectivity* φ *of* $\mathrm{PG}(1, E)$ *such that* $L_T^{\varphi} = L'_T$*.*

Proof.

"$\Leftarrow$" See M. Lavrauw, J. Sheekey, C. Zanella [15, Cor. 18] or [9].

"$\Rightarrow$" For the most part, the proof can be done neatly in $\mathrm{PG}(1, E)$ using the representation of projectivities in terms of $\mathrm{GL}_2(E)$ ...

Main result

Theorem (H. H., C. Zanella [9])

A scattered linear set of $\mathrm{PG}(1, q^t)$, $t \geq 3$, *arising from* $T \in \mathrm{PG}(1, E)$ *is of pseudoregulus type if, and only if, there exists a projectivity* φ *of* $\mathrm{PG}(1, E)$ *such that* $L_T^{\varphi} = L'_T$.

Proof.

"$\Leftarrow$" See M. Lavrauw, J. Sheekey, C. Zanella [15, Cor. 18] or [9].

"$\Rightarrow$" For the most part, the proof can be done neatly in $\mathrm{PG}(1, E)$ using the representation of projectivities in terms of $\mathrm{GL}_2(E)$ ...

Essence: We establish the existence of a cyclic group of projectivities of $\mathrm{PG}(1, E)$ acting regularly on L_T and fixing L'_T pointwise.

References

The list of references contains also relevant work that went uncited on the previous slides.

[1] A. Blunck, Regular spreads and chain geometries. *Bull. Belg. Math. Soc. Simon Stevin* **6** (1999), 589–603.

[2] A. Blunck, H. Havlicek, Extending the concept of chain geometry. *Geom. Dedicata* **83** (2000), 119–130.

[3] A. Blunck, A. Herzer, *Kettengeometrien – Eine Einführung*. Shaker Verlag, Aachen 2005.

[4] B. Csajbók, C. Zanella, On scattered linear sets of pseudoregulus type in $\mathrm{PG}(1, q^t)$. *Finite Fields Appl.* **41** (2016), 34–54.

[5] B. Csajbók, C. Zanella, On the equivalence of linear sets. *Des. Codes Cryptogr.* **81** (2016), 269–281.

References (cont.)

[6] G. Donati, N. Durante, Scattered linear sets generated by collineations between pencils of lines. *J. Algebraic Combin.* **40** (2014), 1121–1134.

[7] R. H. Dye, Spreads and classes of maximal subgroups of $\mathrm{GL}_n(q)$, $\mathrm{SL}_n(q)$,, $\mathrm{PGL}_n(q)$ and $\mathrm{PSL}_n(q)$. *Ann. Mat. Pura Appl. (4)* **158** (1991), 33–50.

[8] H. Havlicek, Divisible designs, Laguerre geometry, and beyond. *J. Math. Sci. (N.Y.)* **186** (2012), 882–926.

[9] H. Havlicek, C. Zanella, Linear sets in the projective line over the endomorphism ring of a finite field. *J. Algebraic Combin.* **46** (2017), 297–312.

[10] A. Herzer, Chain geometries. In: F. Buekenhout, editor, *Handbook of Incidence Geometry*, 781–842, Elsevier, Amsterdam 1995.

References (cont.)

[11] X. Hubaut, Algèbres projectives. *Bull. Soc. Math. Belg.* **17** (1965), 495–502.

[12] N. Knarr, *Translation Planes*, volume 1611 of *Lecture Notes in Mathematics*. Springer, Berlin 1995.

[13] S. Lang, *Algebra*. Addison-Wesley, Reading, MA 1993.

[14] M. Lavrauw, Scattered spaces in Galois geometry. In: *Contemporary developments in finite fields and applications*, 195–216, World Sci. Publ., Hackensack, NJ 2016.

[15] M. Lavrauw, J. Sheekey, C. Zanella, On embeddings of minimum dimension of $\mathrm{PG}(n,q) \times \mathrm{PG}(n,q)$. *Des. Codes Cryptogr.* **74** (2015), 427–440.

[16] M. Lavrauw, G. Van de Voorde, On linear sets on a projective line. *Des. Codes Cryptogr.* **56** (2010), 89–104.

References (cont.)

[17] M. Lavrauw, G. Van de Voorde, Field reduction and linear sets in finite geometry. In: *Topics in finite fields*, volume 632 of *Contemp. Math.*, 271–293, Amer. Math. Soc., Providence, RI 2015.

[18] M. Lavrauw, C. Zanella, Subgeometries and linear sets on a projective line. *Finite Fields Appl.* **34** (2015), 95–106.

[19] M. Lavrauw, C. Zanella, Subspaces intersecting each element of a regulus in one point, André-Bruck-Bose representation and clubs. *Electron. J. Combin.* **23** (2016), Paper 1.37, 11.

[20] G. Lunardon, G. Marino, O. Polverino, R. Trombetti, Maximum scattered linear sets of pseudoregulus type and the Segre variety $\mathcal{S}_{n,n}$. *J. Algebraic Combin.* **39** (2014), 807–831.

[21] G. Lunardon, O. Polverino, Blocking sets and derivable partial spreads. *J. Algebraic Combin.* **14** (2001), 49–56.

References (cont.)

[22] O. Polverino, Linear sets in finite projective spaces. *Discrete Math.* **310** (2010).

[23] G. Van de Voorde, Desarguesian spreads and field reduction for elements of the semilinear group. *Linear Algebra Appl.* **507** (2016), 96–120.

[24] Z.-X. Wan, *Geometry of Matrices*. World Scientific, Singapore 1996.