Pre-sympletic Semifields

Giovanni Longobardi

University of Naples 'Federico II'

Joint work with Guglielmo Lunardon

Finite Geometries Fifth Irsee Conference

10 - 16 September 2017

Contents

Spread

$$V = V(2n, \mathbb{F}_q) = V(2n, q)$$

Spread

$$V = V(2n, \mathbb{F}_q) = V(2n, q)$$

A **spread** $\mathcal{S}$ of V is a set of n-dimensional subspaces such that any vector different from zero belongs to exactly one element of $\mathcal{S}$.

Spread

$$V = V(2n, \mathbb{F}_q) = V(2n, q)$$

A **spread** $\mathcal{S}$ of V is a set of n-dimensional subspaces such that any vector different from zero belongs to exactly one element of $\mathcal{S}$.

Any spread of V determines a translation plane $\mathcal{U}(\mathcal{S})$ whose points are the non zero vectors of V and whose lines are the cosets of the elements of $\mathcal{S}$.

Spread

$$V = V(2n, \mathbb{F}_q) = V(2n, q)$$

A **spread** $\mathcal{S}$ of V is a set of n-dimensional subspaces such that any vector different from zero belongs to exactly one element of $\mathcal{S}$.

Any spread of V determines a translation plane $\mathcal{U}(\mathcal{S})$ whose points are the non zero vectors of V and whose lines are the cosets of the elements of $\mathcal{S}$.

The **kernel** of $\mathcal{U}(\mathcal{S})$ is the field of all $\mathbb{F}_q$-endomorphisms of V fixing all the element of $\mathcal{S}$.

Spread

$\mathcal{S}$ and $\mathcal{S}'$ are **isomorphic** $\iff \exists \tau \in P\Gamma L(2n, q)$ s. t. $\mathcal{S}^\tau = \mathcal{S}'$.

Spread

$\mathcal{S}$ and $\mathcal{S}'$ are **isomorphic** $\iff \exists \tau \in P\Gamma L(2n, q)$ s. t. $\mathcal{S}^\tau = \mathcal{S}'$.

A spread $\mathcal{S}$ of $PG(2n-1, q)$ is a **sympletic spread** with respect to a non singular sympletic polarity $\perp$ of $PG(2n-1, q)$ when all subspaces of $\mathcal{S}$ are totally isotropic with respect to $\perp$.

Finite Semifield

A **finite semifield** $\mathbb{S}$ is an algebra at least two elements, and two binary operations $+$ and $\star$, satisfying the following axioms:

Finite Semifield

A **finite semifield** $\mathbb{S}$ is an algebra at least two elements, and two binary operations + and $\star$, satisfying the following axioms:

(1) $(\mathbb{S}, +)$ is an abelian group.

Finite Semifield

A **finite semifield** $\mathbb{S}$ is an algebra at least two elements, and two binary operations + and $\star$, satisfying the following axioms:

(1) $(\mathbb{S}, +)$ is an abelian group.

(2) $x \star (y + z) = x \star y + x \star z$ and
$(x + y) \star z = x \star z + y \star z, \quad \forall x, y, z \in \mathbb{S}$.

Finite Semifield

A **finite semifield** $\mathbb{S}$ is an algebra at least two elements, and two binary operations + and $\star$, satisfying the following axioms:

(1) $(\mathbb{S}, +)$ is an abelian group.

(2) $x \star (y + z) = x \star y + x \star z$ and
$(x + y) \star z = x \star z + y \star z, \quad \forall x, y, z \in \mathbb{S}$.

(3) $x \star y = 0 \Rightarrow x = 0$ or $y = 0$.

Finite Semifield

A **finite semifield** $\mathbb{S}$ is an algebra at least two elements, and two binary operations + and $\star$, satisfying the following axioms:

(1) $(\mathbb{S}, +)$ is an abelian group.

(2) $x \star (y + z) = x \star y + x \star z$ and
$(x + y) \star z = x \star z + y \star z, \quad \forall x, y, z \in \mathbb{S}$.

(3) $x \star y = 0 \Rightarrow x = 0$ or $y = 0$.

(4) $\exists 1 \in \mathbb{S}$ s.t. $1 \star x = x \star 1 = x \quad \forall x \in \mathbb{S}$.

Finite Semifield

A **finite semifield** $\mathbb{S}$ is an algebra at least two elements, and two binary operations + and $\star$, satisfying the following axioms:

(1) $(\mathbb{S}, +)$ is an abelian group.

(2) $x \star (y + z) = x \star y + x \star z$ and $(x + y) \star z = x \star z + y \star z, \quad \forall x, y, z \in \mathbb{S}$.

(3) $x \star y = 0 \Rightarrow x = 0$ or $y = 0$.

(4) $\exists 1 \in \mathbb{S}$ s.t. $1 \star x = x \star 1 = x \quad \forall x \in \mathbb{S}$.

An algebra satisfying all the axioms of semifield except (4) is called a **presemifield**.

The subsets

Finite Semifield

The subsets

- $\mathcal{N}_l = \{x \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z), \ \forall y, z \in \mathbb{S}\}$

Finite Semifield

The subsets

- $\mathcal{N}_l = \{x \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z), \;\forall y, z \in \mathbb{S}\}$
- $\mathcal{N}_m = \{y \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z), \forall x, z \in \mathbb{S}\}$

Finite Semifield

The subsets

- $\mathcal{N}_l = \{x \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z),\ \forall y, z \in \mathbb{S}\}$
- $\mathcal{N}_m = \{y \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z), \forall x, z \in \mathbb{S}\}$
- $\mathcal{N}_r = \{z \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z),\ \forall x, y \in \mathbb{S}\}$

The subsets

- $\mathcal{N}_l = \{x \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z), \ \forall y, z \in \mathbb{S}\}$
- $\mathcal{N}_m = \{y \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z), \forall x, z \in \mathbb{S}\}$
- $\mathcal{N}_r = \{z \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z), \ \forall x, y \in \mathbb{S}\}$
- $\mathcal{Z} = \{x \in \mathcal{N}_l \cap \mathcal{N}_m \cap \mathcal{N}_r \,|\, x \star y = y \star x, \ \forall y \in \mathbb{S}\}$

Finite Semifield

The subsets

- $\mathcal{N}_l = \{x \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z),\ \forall y, z \in \mathbb{S}\}$
- $\mathcal{N}_m = \{y \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z), \forall x, z \in \mathbb{S}\}$
- $\mathcal{N}_r = \{z \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z),\ \forall x, y \in \mathbb{S}\}$
- $\mathcal{Z} = \{x \in \mathcal{N}_l \cap \mathcal{N}_m \cap \mathcal{N}_r \,|\, x \star y = y \star x,\ \forall y \in \mathbb{S}\}$

are called the **left nucleus**, **middle nucleus**, **right nucleus** and **center** of $\mathbb{S}$, respectively.

Finite Semifield

The subsets

- $\mathcal{N}_l = \{x \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z),\ \forall y, z \in \mathbb{S}\}$
- $\mathcal{N}_m = \{y \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z), \forall x, z \in \mathbb{S}\}$
- $\mathcal{N}_r = \{z \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z),\ \forall x, y \in \mathbb{S}\}$
- $\mathcal{Z} = \{x \in \mathcal{N}_l \cap \mathcal{N}_m \cap \mathcal{N}_r \,|\, x \star y = y \star x,\ \forall y \in \mathbb{S}\}$

are called the **left nucleus**, **middle nucleus**, **right nucleus** and **center** of $\mathbb{S}$, respectively.

$\mathbb{S} = (\mathbb{F}_{q^n}, +, \star)$ is **central** over $\mathbb{F}_s$, $q = s^h$, if

Finite Semifield

The subsets

- $\mathcal{N}_l = \{x \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z),\ \forall y, z \in \mathbb{S}\}$
- $\mathcal{N}_m = \{y \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z), \forall x, z \in \mathbb{S}\}$
- $\mathcal{N}_r = \{z \in \mathbb{S} \,|\, (x \star y) \star z = x \star (y \star z),\ \forall x, y \in \mathbb{S}\}$
- $\mathcal{Z} = \{x \in \mathcal{N}_l \cap \mathcal{N}_m \cap \mathcal{N}_r \,|\, x \star y = y \star x,\ \forall y \in \mathbb{S}\}$

are called the **left nucleus**, **middle nucleus**, **right nucleus** and **center** of $\mathbb{S}$, respectively.

$\mathbb{S} = (\mathbb{F}_{q^n}, +, \star)$ is **central** over $\mathbb{F}_s$, $q = s^h$, if

$$\lambda(a \star b) = (\lambda a) \star b = a \star (\lambda b)\ \forall a, b \in \mathbb{S}, \forall \lambda \in \mathbb{F}_s$$

If L_b is the map of $\mathbb{S}$ in itself defined by $L_b : a \to a \star b$, let $\mathbb{F}_s$ be the maximal subfield of $\mathbb{S}$ s. t. all the L_b are $\mathbb{F}_s$-linear maps.

Semifield Spread

If L_b is the map of $\mathbb{S}$ in itself defined by $L_b : a \to a \star b$, let $\mathbb{F}_s$ be the maximal subfield of $\mathbb{S}$ s. t. all the L_b are $\mathbb{F}_s$-linear maps.

Then $V = \mathbb{S} \oplus \mathbb{S}$ is a vector space over $\mathbb{F}_s$,

If L_b is the map of $\mathbb{S}$ in itself defined by $L_b : a \to a \star b$, let $\mathbb{F}_s$ be the maximal subfield of $\mathbb{S}$ s. t. all the L_b are $\mathbb{F}_s$-linear maps.

Then $V = \mathbb{S} \oplus \mathbb{S}$ is a vector space over $\mathbb{F}_s$,

$$S_\infty = 0 \oplus \mathbb{S}$$
$$S_b = \{(x, x \star b) \mid x \in \mathbb{S}\} \quad b \in \mathbb{S}$$

Semifield Spread

If L_b is the map of $\mathbb{S}$ in itself defined by $L_b : a \to a \star b$, let $\mathbb{F}_s$ be the maximal subfield of $\mathbb{S}$ s. t. all the L_b are $\mathbb{F}_s$-linear maps.

Then $V = \mathbb{S} \oplus \mathbb{S}$ is a vector space over $\mathbb{F}_s$,

$$S_\infty = 0 \oplus \mathbb{S}$$
$$S_b = \{(x, x \star b) \mid x \in \mathbb{S}\} \quad b \in \mathbb{S}$$

are V's n-dimensional subspaces.

Semifield Spread

If L_b is the map of $\mathbb{S}$ in itself defined by $L_b : a \to a \star b$, let $\mathbb{F}_s$ be the maximal subfield of $\mathbb{S}$ s. t. all the L_b are $\mathbb{F}_s$-linear maps.

Then $V = \mathbb{S} \oplus \mathbb{S}$ is a vector space over $\mathbb{F}_s$,

$$S_\infty = 0 \oplus \mathbb{S}$$
$$S_b = \{(x, x \star b) \mid x \in \mathbb{S}\} \quad b \in \mathbb{S}$$

are V's n-dimensional subspaces.

- $\mathcal{S} = \{S_b \mid b \in \mathbb{S} \cup \{\infty\}\}$

Semifield Spread

If L_b is the map of $\mathbb{S}$ in itself defined by $L_b : a \to a \star b$, let $\mathbb{F}_s$ be the maximal subfield of $\mathbb{S}$ s. t. all the L_b are $\mathbb{F}_s$-linear maps.

Then $V = \mathbb{S} \oplus \mathbb{S}$ is a vector space over $\mathbb{F}_s$,

$$\begin{array}{l} S_\infty = 0 \oplus \mathbb{S} \\ S_b = \{(x, x \star b) \mid x \in \mathbb{S}\} \quad b \in \mathbb{S} \end{array}$$

are V's n-dimensional subspaces.

- $\mathcal{S} = \{S_b \mid b \in \mathbb{S} \cup \{\infty\}\}$
- $\mathcal{U} = \mathcal{U}(\mathcal{S}) = \mathcal{U}(\mathbb{S})$

If L_b is the map of $\mathbb{S}$ in itself defined by $L_b : a \to a \star b$, let $\mathbb{F}_s$ be the maximal subfield of $\mathbb{S}$ s. t. all the L_b are $\mathbb{F}_s$-linear maps.

Then $V = \mathbb{S} \oplus \mathbb{S}$ is a vector space over $\mathbb{F}_s$,

$$S_\infty = 0 \oplus \mathbb{S}$$
$$S_b = \{(x, x \star b) \mid x \in \mathbb{S}\} \quad b \in \mathbb{S}$$

are V's n-dimensional subspaces.

- $\mathcal{S} = \{S_b \mid b \in \mathbb{S} \cup \{\infty\}\}$
- $\mathcal{U} = \mathcal{U}(\mathcal{S}) = \mathcal{U}(\mathbb{S})$
- $\mathbb{S}$ and $\mathbb{S}'$ are **isotopic** $\iff$ $\mathcal{U}(\mathbb{S}) \cong \mathcal{U}(\mathbb{S}')$

Adjoint map and dual semifield

Let $\mathbb{S} = (\mathbb{F}_{q^n}, +, \star)$ a presemifield be.

Adjoint map and dual semifield

Let $\mathbb{S} = (\mathbb{F}_{q^n}, +, \star)$ a presemifield be.
If L is an $\mathbb{F}_q$-linear map of $\mathbb{F}_{q^n}$ in itself, the adjoint $\tilde{L}$ of L with respect to the bilinear form $Tr_q(xy)$ is defined by

$$Tr_q(xL(y)) = Tr_q(\tilde{L}(x)y) \ \forall x, y \in \mathbb{F}_{q^n}$$

Adjoint map and dual semifield

Let $\mathbb{S} = (\mathbb{F}_{q^n}, +, \star)$ a presemifield be.
If L is an $\mathbb{F}_q$-linear map of $\mathbb{F}_{q^n}$ in itself, the adjoint $\tilde{L}$ of L with respect to the bilinear form $Tr_q(xy)$ is defined by

$$Tr_q(xL(y)) = Tr_q(\tilde{L}(x)y) \ \forall x, y \in \mathbb{F}_{q^n}$$

The **dual** of $\mathbb{S}$ is $\mathbb{S}^d = (\mathbb{F}_{q^n}, +, \circ)$ defined by

$$x \circ y = y \star x$$

Linear sets

Let $PG(r-1,q^n) = PG(V,q^n)$ be the projective space over $V(r,q^n)$.

Linear sets

Let $PG(r-1, q^n) = PG(V, q^n)$ be the projective space over $V(r, q^n)$.
- Ω is an $\mathbb{F}_q$-**linear set** if

Linear sets

Let $PG(r-1, q^n) = PG(V, q^n)$ be the projective space over $V(r, q^n)$.

- Ω is an $\mathbb{F}_q$-**linear set** if

$$\langle w \rangle \in \Omega \iff w \in W$$

Linear sets

Let $PG(r-1,q^n) = PG(V,q^n)$ be the projective space over $V(r,q^n)$.

- Ω is an $\mathbb{F}_q$-**linear set** if

$$\langle w \rangle \in \Omega \iff w \in W$$

where W is a $\mathbb{F}_q$-vector subspace of V.

Linear sets

Let $PG(r-1, q^n) = PG(V, q^n)$ be the projective space over $V(r, q^n)$.

- Ω is an $\mathbb{F}_q$-**linear set** if

$$\langle w \rangle \in \Omega \iff w \in W$$

where W is a $\mathbb{F}_q$-vector subspace of V.

$$rk\Omega := rk_{\mathbb{F}_q} W \quad (\Omega\text{'s } \textbf{rank}).$$

Let $PG(r-1, q^n) = PG(V, q^n)$ be the projective space over $V(r, q^n)$.

- Ω is an $\mathbb{F}_q$-**linear set** if

$$\langle w \rangle \in \Omega \iff w \in W$$

where W is a $\mathbb{F}_q$-vector subspace of V.

$$rk\Omega := rk_{\mathbb{F}_q} W \quad (\Omega\text{'s } \textbf{rank}).$$

If Ω has rank r and $\langle W \rangle_{\mathbb{F}_q} = V$,

$$\Omega \cong PG(W, \mathbb{F}_q) = PG(r-1, q)$$

is a **canonical subgeometry** of $PG(r-1, q^n)$.

Linear sets

Let $PG(r-1, q^n) = PG(V, q^n)$ be the projective space over $V(r, q^n)$.
- Ω is an $\mathbb{F}_q$-**linear set** if

$$\langle w \rangle \in \Omega \iff w \in W$$

where W is a $\mathbb{F}_q$-vector subspace of V.

$$rk\Omega := rk_{\mathbb{F}_q} W \quad (\Omega\text{'s } \textbf{rank}).$$

If Ω has rank r and $\langle W \rangle_{\mathbb{F}_q} = V$,

$$\Omega \cong PG(W, \mathbb{F}_q) = PG(r-1, q)$$

is a **canonical subgeometry** of $PG(r-1, q^n)$.

$$\Sigma = \{(x, x^q, \ldots, x^{q^{n-1}}) \in PG(n-1, q^n) \,|\, x \in \mathbb{F}_{q^n}\}$$

Geometric spread set (with respect to Σ) and sympletic cone

Let $\perp$ be the polarity of $\mathbb{P} = PG(n-1, q^n)$ defined by the bilinear form

$$b(\mathbf{x}, \mathbf{y}) = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \quad \forall \mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^n}^n$$

Geometric spread set (with respect to Σ) and sympletic cone

Let $\perp$ be the polarity of $\mathbb{P} = PG(n-1, q^n)$ defined by the bilinear form

$$b(\mathbf{x}, \mathbf{y}) = x_1y_1 + x_2y_2 + \ldots + x_ny_n \quad \forall \mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^n}^n$$

A **geometric spread set** Γ of $\mathbb{P}$ (with respect to Σ) is a $\mathbb{F}_s$-linear set of rank nh, $q = s^h$, s. t.

$$\Gamma^\star = \{(y_1, y_2, \ldots, y_n) \in \mathbb{P} \mid Tr_s(b(\mathbf{x}, \mathbf{y})) = 0 \ \forall \mathbf{x} \in \Gamma\}$$

is disjoint from Σ.

Geometric spread set (with respect to Σ) and sympletic cone

Let $\perp$ be the polarity of $\mathbb{P} = PG(n-1, q^n)$ defined by the bilinear form

$$b(\mathbf{x}, \mathbf{y}) = x_1y_1 + x_2y_2 + \ldots + x_ny_n \quad \forall \mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^n}^n$$

A **geometric spread set** Γ of $\mathbb{P}$ (with respect to Σ) is a $\mathbb{F}_s$-linear set of rank nh, $q = s^h$, s. t.

$$\Gamma^\star = \{(y_1, y_2, \ldots, y_n) \in \mathbb{P} \,|\, Tr_s(b(\mathbf{x}, \mathbf{y})) = 0 \ \forall \mathbf{x} \in \Gamma\}$$

is disjoint from Σ.

Geometric spread set (with respect to Σ) and sympletic cone

Let $\perp$ be the polarity of $\mathbb{P} = PG(n-1, q^n)$ defined by the bilinear form

$$b(\mathbf{x}, \mathbf{y}) = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \quad \forall \mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^n}^n$$

A **geometric spread set** Γ of $\mathbb{P}$ (with respect to Σ) is a $\mathbb{F}_s$-linear set of rank nh, $q = s^h$, s. t.

$$\Gamma^\star = \{(y_1, y_2, \ldots, y_n) \in \mathbb{P} \,|\, Tr_s(b(\mathbf{x}, \mathbf{y})) = 0 \ \forall \mathbf{x} \in \Gamma\}$$

is disjoint from Σ.

Geometric spread set (with respect to Σ) and sympletic cone

Let $\perp$ be the polarity of $\mathbb{P} = PG(n-1, q^n)$ defined by the bilinear form

$$b(\mathbf{x}, \mathbf{y}) = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \quad \forall \mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^n}^n$$

A **geometric spread set** Γ of $\mathbb{P}$ (with respect to Σ) is a $\mathbb{F}_s$-linear set of rank nh, $q = s^h$, s. t.

$$\Gamma^\star = \{(y_1, y_2, \ldots, y_n) \in \mathbb{P} \mid Tr_s(b(\mathbf{x}, \mathbf{y})) = 0 \ \forall \mathbf{x} \in \Gamma\}$$

is disjoint from Σ.

The $\mathbb{F}_q$-linear set of rank $\frac{n(n+1)}{2}$ of $\mathbb{P}$

$$\Omega = \{(\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{P} \mid i = 2, 3, \ldots, n : \beta_i^{q^{n-i+1}} = \beta_{n-i+2}\}$$

is called **sympletic cone** .

Geometric construction

Let $\Gamma = \{(x, f(x)^q, f(x)) : x \in \mathbb{F}_{q^3}\}$ be a geometric spread set of $\mathbb{P} = PG(2, q^3)$ (with respect to Σ).

Geometric construction

Let $\Gamma = \{(x, f(x)^q, f(x)) : x \in \mathbb{F}_{q^3}\}$ be a geometric spread set of $\mathbb{P} = PG(2, q^3)$ (with respect to Σ).

Γ is contained in the sympletic cone Ω.

Geometric construction

Let $\Gamma = \{(x, f(x)^q, f(x)) : x \in \mathbb{F}_{q^3}\}$ be a geometric spread set of $\mathbb{P} = PG(2, q^3)$ (with respect to Σ).

Γ is contained in the sympletic cone Ω.

As before, let $\perp$ be the polarity of $\mathbb{P}$

Geometric construction

Let $\Gamma = \{(x, f(x)^q, f(x)) : x \in \mathbb{F}_{q^3}\}$ be a geometric spread set of $\mathbb{P} = PG(2, q^3)$ (with respect to Σ).

> Γ is contained in the sympletic cone Ω.

As before, let $\perp$ be the polarity of $\mathbb{P}$

- $\Omega^\star = \{(0, \xi^q, -\xi) : \xi \in \mathbb{F}_{q^3}\}$

Geometric construction

Let $\Gamma = \{(x, f(x)^q, f(x)) : x \in \mathbb{F}_{q^3}\}$ be a geometric spread set of $\mathbb{P} = PG(2, q^3)$ (with respect to Σ).

Γ is contained in the sympletic cone Ω.

As before, let $\perp$ be the polarity of $\mathbb{P}$

- $\Omega^\star = \{(0, \xi^q, -\xi) : \xi \in \mathbb{F}_{q^3}\}$
- $\Gamma^\star = \{(\tilde{f}(y), \xi^q, -y - \xi) : y, \xi \in \mathbb{F}_{q^3}\}$

Let $\Gamma = \{(x, f(x)^q, f(x)) : x \in \mathbb{F}_{q^3}\}$ be a geometric spread set of $\mathbb{P} = PG(2, q^3)$ (with respect to Σ).

> Γ is contained in the sympletic cone Ω.

As before, let $\perp$ be the polarity of $\mathbb{P}$

- $\Omega^\star = \{(0, \xi^q, -\xi) : \xi \in \mathbb{F}_{q^3}\}$
- $\Gamma^\star = \{(\tilde{f}(y), \xi^q, -y - \xi) : y, \xi \in \mathbb{F}_{q^3}\}$

where $\tilde{f}(y)$ is the adjoint map of f with respect to the quadratic form $q(\alpha) = Tr_s(\alpha^2)$.

Geometric construction

Let $\Delta := \langle \Sigma, \Omega^\star \rangle$ be, Let $\Delta := \langle \Sigma, \Omega^\star \rangle$ be,

$$P \in (\Delta \setminus \Sigma) \cap r \iff P(x\alpha, 0, x\alpha^{q^2} + x^{q^2}\alpha), \; x \in \mathbb{F}_{q^3}, \, \alpha \in \mathbb{F}^*_{q^3}$$

where $r : x_2 = 0$.

Geometric construction

Let $\Delta := \langle \Sigma, \Omega^\star \rangle$ be,

$$P \in (\Delta \setminus \Sigma) \cap r \iff P(x\alpha, 0, x\alpha^{q^2} + x^{q^2}\alpha),\ x \in \mathbb{F}_{q^3},\ \alpha \in \mathbb{F}^*_{q^3}$$

where $r : x_2 = 0$.

$$\Lambda_\alpha = \{(x\alpha, 0, x\alpha^{q^2} + x^{q^2}\alpha)\ : x \in \mathbb{F}^*_{q^3}\}$$

Geometric construction

Let $\Delta := \langle \Sigma, \Omega^\star \rangle$ be,

$$P \in (\Delta \setminus \Sigma) \cap r \iff P(x\alpha, 0, x\alpha^{q^2} + x^{q^2}\alpha), \;\; x \in \mathbb{F}_{q^3}, \; \alpha \in \mathbb{F}^*_{q^3}$$

where $r : x_2 = 0$.

$$\Lambda_\alpha = \{(x\alpha, 0, x\alpha^{q^2} + x^{q^2}\alpha) \;: x \in \mathbb{F}^*_{q^3}\}$$

$$\Gamma^\star_2 = \Gamma^\star \cap r = \{(-\tilde{f}(y), 0, y) : y \in \mathbb{F}^\star_{q^3}\}.$$

Geometric construction

Let $\Delta := \langle \Sigma, \Omega^\star \rangle$ be,

$$P \in (\Delta \setminus \Sigma) \cap r \iff P(x\alpha, 0, x\alpha^{q^2} + x^{q^2}\alpha), \; x \in \mathbb{F}_{q^3}, \; \alpha \in \mathbb{F}^*_{q^3}$$

where $r : x_2 = 0$.

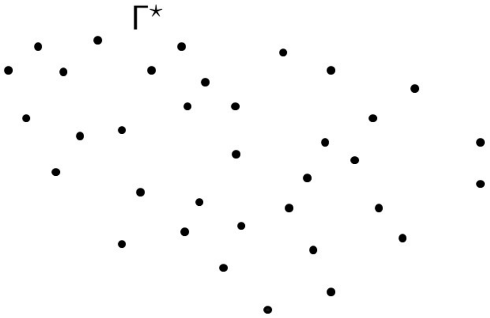
$$\Lambda_\alpha = \{(x\alpha, 0, x\alpha^{q^2} + x^{q^2}\alpha) \; : x \in \mathbb{F}^*_{q^3}\}$$

$$\Gamma^\star_2 = \Gamma^\star \cap r = \{(-\tilde{f}(y), 0, y) : y \in \mathbb{F}^\star_{q^3}\}.$$

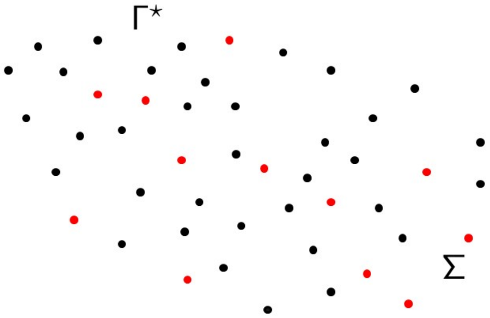
Then

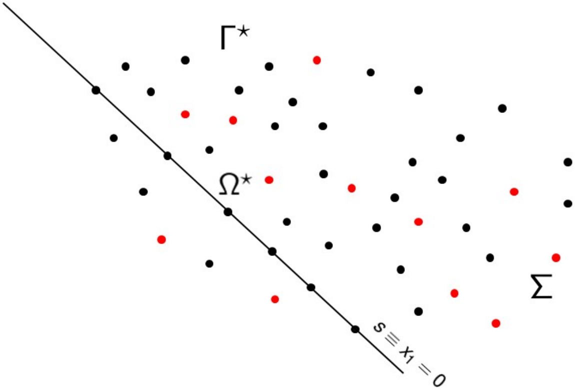
$$\begin{vmatrix} x\alpha & x\alpha^{q^2} + x^{q^2}\alpha \\ -\tilde{f}(y) & y \end{vmatrix} \neq 0$$

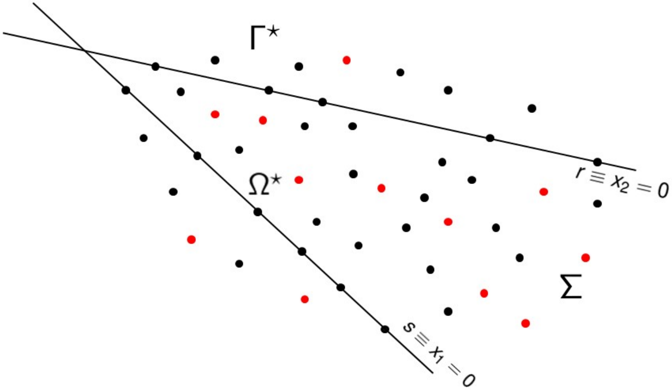
for all $\alpha, x, y \in \mathbb{F}^*_{q^3}$.



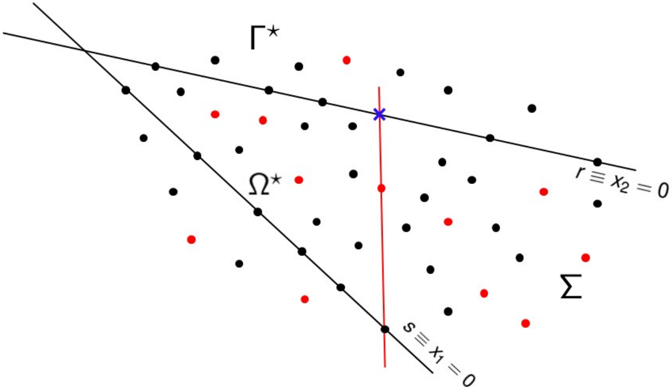
$\Gamma^\star$


$\Gamma^\star$
Σ


Γ*
Ω*
Σ
s ≡ x1 = 0



$\Gamma^\star$
$\Omega^\star$
$r \equiv x_2 = 0$
Σ
$s \equiv x_1 = 0$



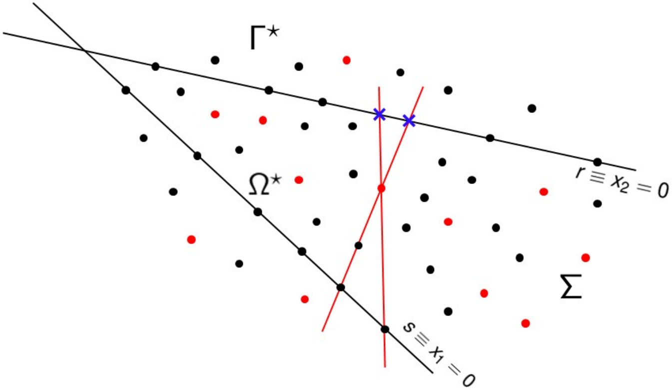
Pre-sympletic Semifields

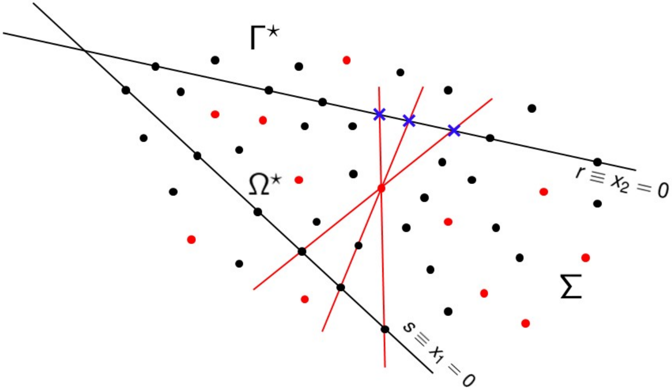
G. Longobardi, G. Lunardon

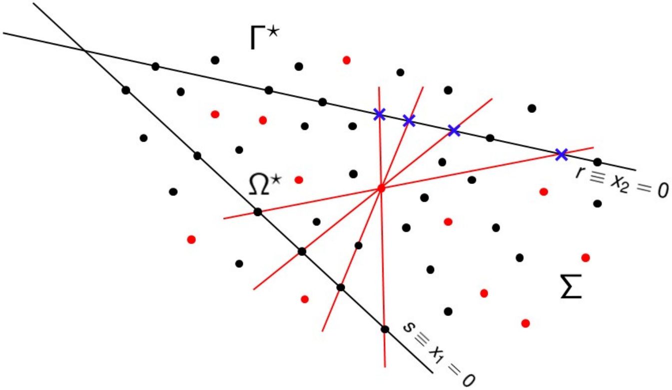
Preliminaries

Geometric construction

Results


$\Gamma^\star$
$\Omega^\star$
$r \equiv x_2 = 0$
$s \equiv x_1 = 0$
Σ


$\Gamma^\star$
$\Omega^\star$
Σ
$r \equiv x_2 = 0$
$s \equiv x_1 = 0$


Γ*
Ω*
Σ
r ≡ x2 = 0
s ≡ x1 = 0

Theorem [L., Lunardon]

Γ is a geometric spread set if and only if, $\mathbb{S}_\alpha = (\mathbb{F}_{q^3}, +, \star_\alpha)$ with multiplication defined by

$$x \star_\alpha y = (\tilde{f}(y)\alpha^{q^2-1} + y)x + \tilde{f}(y)x^{q^2}$$

is, for all $\alpha \in \mathbb{F}^*_{q^3}$, a presemifield central over $\mathbb{F}_s$ and the kernel of the plane $\mathcal{U}_\alpha$ contains $\mathbb{F}_q$.

Theorem [L., Lunardon]

Γ is a geometric spread set if and only if, $\mathbb{S}_\alpha = (\mathbb{F}_{q^3}, +, \star_\alpha)$ with multiplication defined by

$$x \star_\alpha y = (\tilde{f}(y)\alpha^{q^2-1} + y)x + \tilde{f}(y)x^{q^2}$$

is, for all $\alpha \in \mathbb{F}^*_{q^3}$, a presemifield central over $\mathbb{F}_s$ and the kernel of the plane $\mathcal{U}_\alpha$ contains $\mathbb{F}_q$.

Corollary [L., Lunardon]

$\mathbb{F} = (\mathbb{F}_{q^3}, +, \cdot)$ with multiplication defined by

$$x \cdot y = xy + f(y)^q x^q + f(y)x^{q^2}$$

is a sympletic presemifield if and only if $\mathbb{S}_\alpha$ is a presemifield for all $\alpha \in \mathbb{F}^*_{q^3}$.

Results

Theorem [L., Lunardon]

Γ is a geometric spread set if and only if, $\mathbb{S}_\alpha = (\mathbb{F}_{q^3}, +, \star_\alpha)$ with multiplication defined by

$$x \star_\alpha y = (\tilde{f}(y)\alpha^{q^2-1} + y)x + \tilde{f}(y)x^{q^2}$$

is, for all $\alpha \in \mathbb{F}^*_{q^3}$, a presemifield central over $\mathbb{F}_s$ and the kernel of the plane $\mathcal{U}_\alpha$ contains $\mathbb{F}_q$.

Corollary [L., Lunardon]

$\mathbb{F} = (\mathbb{F}_{q^3}, +, \cdot)$ with multiplication defined by

$$x \cdot y = xy + f(y)^q x^q + f(y)x^{q^2}$$

is a sympletic presemifield if and only if $\mathbb{S}_\alpha$ is a presemifield for all $\alpha \in \mathbb{F}^*_{q^3}$.

Remark: $|\{\mathbb{S}_\alpha\}_{\alpha \in \mathbb{F}^*_{q^3}}| = q^2 + q + 1$.

Even characteristic Results

$\Gamma_f = \{(x, f(x)^q, f(x)) : x \in \mathbb{F}_{q^3}\}$, with $q = 2^h$,

$$f : x \in \mathbb{F}_{q^3} \to \sqrt{x + x^{q^2}} \in \mathbb{F}_{q^3}$$

$$\Gamma_f = \{(x, f(x)^q, f(x)) : x \in \mathbb{F}_{q^3}\}, \text{ with } q = 2^h,$$

$$f : x \in \mathbb{F}_{q^3} \to \sqrt{x + x^{q^2}} \in \mathbb{F}_{q^3}$$

Theorem. [Bader, Lunardon (2015)]

Γ_f defines a sympletic presemifield of order q^3.

Even characteristic Results

$\Gamma_f = \{(x, f(x)^q, f(x)) : x \in \mathbb{F}_{q^3}\}$, with $q = 2^h$,

$$f : x \in \mathbb{F}_{q^3} \to \sqrt{x + x^{q^2}} \in \mathbb{F}_{q^3}$$

Theorem. [Bader, Lunardon (2015)]

Γ_f defines a sympletic presemifield of order q^3.

Then, for all $\alpha \in \mathbb{F}^*_{q^3}$, $\mathbb{S}_\alpha = (\mathbb{F}_{q^3}, +, \star_\alpha)$, with multiplication defined by

$\Gamma_f = \{(x, f(x)^q, f(x)) : x \in \mathbb{F}_{q^3}\}$, with $q = 2^h$,

$$f : x \in \mathbb{F}_{q^3} \to \sqrt{x + x^{q^2}} \in \mathbb{F}_{q^3}$$

Theorem. [Bader, Lunardon (2015)]

Γ_f defines a sympletic presemifield of order q^3.

Then, for all $\alpha \in \mathbb{F}^*_{q^3}$, $\mathbb{S}_\alpha = (\mathbb{F}_{q^3}, +, \star_\alpha)$, with multiplication defined by

$$x \star_\alpha y = ((y + y^q)^2 \alpha^{q^2-1} + y)x + (y + y^q)^2 x^{q^2}$$

$\Gamma_f = \{(x, f(x)^q, f(x)) : x \in \mathbb{F}_{q^3}\}$, with $q = 2^h$,

$$f : x \in \mathbb{F}_{q^3} \to \sqrt{x + x^{q^2}} \in \mathbb{F}_{q^3}$$

Theorem. [Bader, Lunardon (2015)]

Γ_f defines a sympletic presemifield of order q^3.

Then, for all $\alpha \in \mathbb{F}^*_{q^3}$, $\mathbb{S}_\alpha = (\mathbb{F}_{q^3}, +, \star_\alpha)$, with multiplication defined by

$$x \star_\alpha y = ((y + y^q)^2 \alpha^{q^2-1} + y)x + (y + y^q)^2 x^{q^2}$$

is a presemifield that, up to isotopy, has:

$\Gamma_f = \{(x, f(x)^q, f(x)) : x \in \mathbb{F}_{q^3}\}$, with $q = 2^h$,

$$f : x \in \mathbb{F}_{q^3} \to \sqrt{x + x^{q^2}} \in \mathbb{F}_{q^3}$$

Theorem. [Bader, Lunardon (2015)]

Γ_f defines a sympletic presemifield of order q^3.

Then, for all $\alpha \in \mathbb{F}^*_{q^3}$, $\mathbb{S}_\alpha = (\mathbb{F}_{q^3}, +, \star_\alpha)$, with multiplication defined by

$$x \star_\alpha y = ((y + y^q)^2 \alpha^{q^2-1} + y)x + (y + y^q)^2 x^{q^2}$$

is a presemifield that, up to isotopy, has:

- $\mathcal{N}_l = \mathbb{F}_q$

Even characteristic Results

$\Gamma_f = \{(x, f(x)^q, f(x)) : x \in \mathbb{F}_{q^3}\}$, with $q = 2^h$,

$$f : x \in \mathbb{F}_{q^3} \to \sqrt{x + x^{q^2}} \in \mathbb{F}_{q^3}$$

Theorem. [Bader, Lunardon (2015)]

Γ_f defines a sympletic presemifield of order q^3.

Then, for all $\alpha \in \mathbb{F}^*_{q^3}$, $\mathbb{S}_\alpha = (\mathbb{F}_{q^3}, +, \star_\alpha)$, with multiplication defined by

$$x \star_\alpha y = ((y + y^q)^2 \alpha^{q^2-1} + y)x + (y + y^q)^2 x^{q^2}$$

is a presemifield that, up to isotopy, has:

- $\mathcal{N}_l = \mathbb{F}_q$
- $\mathcal{Z} = \mathbb{F}_2$

Even characteristic Results

Known semifields of order q^3, $q = 2^h$, with geometric spread sets on a line are:

Even characteristic Results

Known semifields of order q^3, $q = 2^h$, with geometric spread sets on a line are:

- **Fields**;
- **Generalized Twisted fields** with center of order q.

Vielen Dank für Ihre Aufmerksamkeit!