Finite semifields and nonsingular tensors

Michel Lavrauw

Finite Geometries, Third Irsee Conference
June 10-25, 2011

Finite Semifield

A finite semifield $\mathbb{S}$ is a finite division algebra, which is not necessarily associative

Finite Semifield

A finite semifield $\mathbb{S}$ is a finite division algebra, which is not necessarily associative , i.e., $(\mathbb{S}, +, \circ)$ satisfying the following axioms:

(S1) $(\mathbb{S}, +)$ is a finite group

Finite Semifield

A finite semifield $\mathbb{S}$ is a finite division algebra, which is not necessarily associative , i.e., $(\mathbb{S}, +, \circ)$ satisfying the following axioms:

(S1) $(\mathbb{S}, +)$ is a finite group

(S2) Left and right distributive laws hold

- $\forall x, y, z \in \mathbb{S} \ : \ x \circ (y + z) = x \circ y + x \circ z$
- $\forall x, y, z \in \mathbb{S} \ : \ (x + y) \circ z = x \circ z + y \circ z$

Finite Semifield

A finite semifield $\mathbb{S}$ is a finite division algebra, which is not necessarily associative , i.e., $(\mathbb{S}, +, \circ)$ satisfying the following axioms:

(S1) $(\mathbb{S}, +)$ is a finite group

(S2) Left and right distributive laws hold

(S3) $(\mathbb{S}, \circ)$ has no zero-divisors

- $\forall x, y \in \mathbb{S} \ : \ x \circ y = 0 \Rightarrow x = 0$ or $y = 0$

Finite Semifield

A finite semifield $\mathbb{S}$ is a finite division algebra, which is not necessarily associative , i.e., $(\mathbb{S}, +, \circ)$ satisfying the following axioms:

(S1) $(\mathbb{S}, +)$ is a finite group

(S2) Left and right distributive laws hold

(S3) $(\mathbb{S}, \circ)$ has no zero-divisors

(S4) $(\mathbb{S}, \circ)$ has a unit

- $\exists u \in \mathbb{S}, \forall x \in \mathbb{S} \ : \ x \circ u = u \circ x = x,$

Finite Semifield

A finite semifield $\mathbb{S}$ is a finite division algebra, which is not necessarily associative , i.e., $(\mathbb{S}, +, \circ)$ satisfying the following axioms:

(S1) $(\mathbb{S}, +)$ is a finite group

(S2) Left and right distributive laws hold

(S3) $(\mathbb{S}, \circ)$ has no zero-divisors

(S4) $(\mathbb{S}, \circ)$ has a unit

(without (S4) $\rightarrow$ pre-semifield)

From a pre-semifield to a semifield

Let $(\mathbb{S}, \circ)$ be a pre-semifield and $0 \neq u \in \mathbb{S}$.

Define a new multiplication:

$$(a \circ u) * (u \circ b) = a \circ b.$$

Then $(\mathbb{S}, *)$ is a semifield, with unit $u \circ u$.

Examples

Examples

- A finite field is a finite semifield.

Examples

- A finite field is a finite semifield.
- Proper example of odd order q^{2k} (L. E. Dickson 1906)

$$\mathbb{S}_D \; : \; (\mathbb{F}_{q^k}^2, +, \circ) \begin{cases} (x,y)+(u,v) & = (x+u, y+v) \\ (x,y)\circ(u,v) & = (xu+\alpha y^q v^q, xv+yu) \end{cases}$$

where α is a non-square in $\mathbb{F}_{q^k}$.

Examples

- A finite field is a finite semifield.
- Proper example of odd order q^{2k} (L. E. Dickson 1906)

$$\mathbb{S}_D \;:\; (\mathbb{F}_{q^k}^2, +, \circ) \begin{cases} (x,y)+(u,v) & = (x+u, y+v) \\ (x,y)\circ(u,v) & = (xu+\alpha y^q v^q, xv+yu) \end{cases}$$

where α is a non-square in $\mathbb{F}_{q^k}$.

$\rightarrow$ Let's prove (S3): no zero divisors.

Examples

- A finite field is a finite semifield.
- Proper example of odd order q^{2k} (L. E. Dickson 1906)

$$\mathbb{S}_D \ : \ (\mathbb{F}_{q^k}^2, +, \circ) \begin{cases} (x,y)+(u,v) & = (x+u, y+v) \\ (x,y)\circ(u,v) & = (xu+\alpha y^q v^q, xv+yu) \end{cases}$$

where α is a non-square in $\mathbb{F}_{q^k}$.

$\rightarrow$ Let's prove (S3): no zero divisors. Suppose $(x,y)\circ(u,v)=(0,0)$. If $u=0$ or $v=0$, then $(u,v)=(0,0)$. If $u\neq 0\neq v$, then

$$\begin{cases} xu+\alpha y^q v^q & = 0 \\ xv+yu & = 0 \end{cases} \Rightarrow \begin{cases} xuv+\alpha y^q v^{q+1} & = 0 \\ xvu+yu^2 & = 0 \end{cases}$$

If $y\neq 0$ then $\alpha y^{q-1}v^{q+1}=u^2$, a contradiction. Hence $y=0 \Rightarrow (x,y)=(0,0)$.

Examples

- A finite field is a finite semifield.
- Proper example of odd order q^{2k} (L. E. Dickson 1906)

$$\mathbb{S}_D \ : \ (\mathbb{F}_{q^k}^2, +, \circ) \begin{cases} (x,y)+(u,v) & = (x+u, y+v) \\ (x,y)\circ(u,v) & = (xu+\alpha y^q v^q, xv+yu) \end{cases}$$

  where α is a non-square in $\mathbb{F}_{q^k}$.
  Notice: $\mathbb{S}_D$ is commutative, but not associative.
- Generalized twisted fields (A. A. Albert 1961):

$$\mathbb{S}_{GT} \ : \ (\mathbb{F}_{q^n}, +, \circ) \text{ with } x \circ y = xy - \eta x^\alpha y^\beta,$$

  $\alpha, \beta \in Aut(\mathbb{F}_{q^n})$, $Fix(\alpha) = Fix(\beta) = \mathbb{F}_q$, where

$$\eta \in \mathbb{F}_{q^n} \setminus \{x^{\alpha-1} y^{\beta-1} : x, y \in \mathbb{F}_{q^n}\}$$

The name semifields

- Dickson (1906): "Linear algebras in which division is always uniquely possible"

The name semifields

- Dickson (1906): "Linear algebras in which division is always uniquely possible"
- Dickson (1935): " Linear algebras in which associativity is not assumed"

The name semifields

- Dickson (1906): "Linear algebras in which division is always uniquely possible"
- Dickson (1935): " Linear algebras in which associativity is not assumed"
- Albert (1952): "On non-associative division algebras"

The name semifields

- Dickson (1906): “Linear algebras in which division is always uniquely possible”
- Dickson (1935): “ Linear algebras in which associativity is not assumed”
- Albert (1952): “On non-associative division algebras”
- Hughes-Kleinfeld (1960): “Semi-nuclear extensions of Galois fields”

The name semifields

- Dickson (1906): "Linear algebras in which division is always uniquely possible"
- Dickson (1935): " Linear algebras in which associativity is not assumed"
- Albert (1952): "On non-associative division algebras"
- Hughes-Kleinfeld (1960): "Semi-nuclear extensions of Galois fields"
- Knuth (1965):

The name semifields

- Dickson (1906): "Linear algebras in which division is always uniquely possible"
- Dickson (1935): " Linear algebras in which associativity is not assumed"
- Albert (1952): "On non-associative division algebras"
- Hughes-Kleinfeld (1960): "Semi-nuclear extensions of Galois fields"
- Knuth (1965): "We are concerned with a certain type of algebraic system, called a semifield. Such a system has several names in the literature, where it is called, for example, a "nonassociative division ring" or a "distributive quasifield". Since these terms are rather lengthy, and since we make frequent reference to such systems in this paper, the more convenient name semifield will be used."

Since 1965, people have been using the name semifields.

Classification results*

* without assumptions on the nuclei

Classification results*

- A two-dimensional finite semifield is a finite field (Dickson 1906)
- A three-dimensional finite semifield is a twisted field or a field (Menichetti 1977) (Conjectured by Kaplansky)
- The smallest nonassociative semifield has size 16, and semifields have been classified by computer up to order 243 (Rúa-Combarro 2010)

* without assumptions on the nuclei

Translation planes from a semifield $\mathbb{S}$

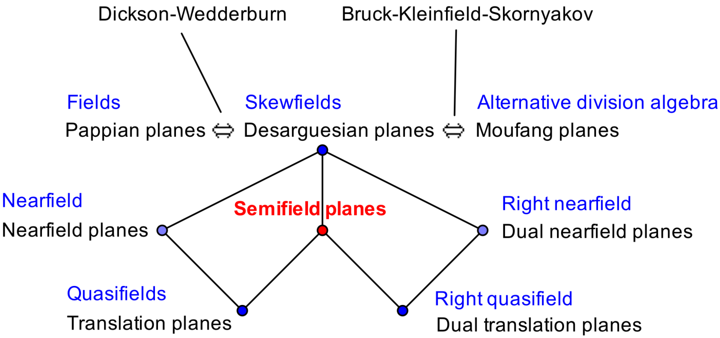
$(\mathbb{S}, \circ) \to$ projective plane $\pi(\mathbb{S}) := (\mathcal{P}, \mathcal{L}, \mathcal{I})$

- $\mathcal{P}$: points (a, b, c), i.e. $(0, 0, 1)$, $(0, 1, c)$, or $(1, b, c)$
- $\mathcal{L}$: lines $[x, y, z]$, i.e. $[0, 0, 1]$, $[0, 1, z]$, or $[1, y, z]$
- Incidence: $(a, b, c)\mathcal{I}[x, y, z] \Leftrightarrow az = b \circ y + cx$

Theorem

The incidence structure $\pi(\mathbb{S})$ is a projective plane. Moreover, it is a translation plane AND a its dual is also a translation plane.

Types of finite translation planes



[Hughes - Piper, Projective Planes, Springer, 1973]

Isotopism classes $\leftrightarrow$ Isomorphism classes

Isotopism classes $\leftrightarrow$ Isomorphism classes

Theorem (Albert 1960)

Two semifield planes are isomorphic if and only if the corresponding semifields are isotopic.

Isotopism classes $\leftrightarrow$ Isomorphism classes

Theorem (Albert 1960)

Two semifield planes are isomorphic if and only if the corresponding semifields are isotopic.

- An isotopism from $(\mathbb{S}, \circ)$ to $(\mathbb{S}', \circ')$ is a triple (F, G, H) of bijections from $\mathbb{S}$ to $\mathbb{S}'$, linear over the characteristic field of $\mathbb{S}$, such that
$$a^F \circ' b^G = (a \circ b)^H$$

Isotopism classes $\leftrightarrow$ Isomorphism classes

Theorem (Albert 1960)

Two semifield planes are isomorphic if and only if the corresponding semifields are isotopic.

- An isotopism from $(\mathbb{S}, \circ)$ to $(\mathbb{S}', \circ')$ is a triple (F, G, H) of bijections from $\mathbb{S}$ to $\mathbb{S}'$, linear over the characteristic field of $\mathbb{S}$, such that
$$a^F \circ' b^G = (a \circ b)^H$$
- If such an isotopism exists, then $\mathbb{S}$ and $\mathbb{S}'$ are called isotopic.

Isotopism classes $\leftrightarrow$ Isomorphism classes

Theorem (Albert 1960)

Two semifield planes are isomorphic if and only if the corresponding semifields are isotopic.

- An isotopism from $(\mathbb{S}, \circ)$ to $(\mathbb{S}', \circ')$ is a triple (F, G, H) of bijections from $\mathbb{S}$ to $\mathbb{S}'$, linear over the characteristic field of $\mathbb{S}$, such that
$$a^F \circ' b^G = (a \circ b)^H$$
- If such an isotopism exists, then $\mathbb{S}$ and $\mathbb{S}'$ are called isotopic.
- Semifield $\mathbb{S} \longrightarrow$ isotopism class $[\mathbb{S}]$

From a pre-semifield to a semifield

Let $\mathbb{S}, \circ$ be a pre-semifield and $0 \neq u \in \mathbb{S}$.

Define a new multiplication:

$$(a \circ u) * (u \circ b) = a \circ b.$$

Then $(\mathbb{S}, *)$ is a semifield isotopic to the pre-semifield $(\mathbb{S}, \circ)$:

$$a^{R_u} \circ b^{L_u} = a \circ b.$$

(Isotopism (R_u, L_u, id))

Nuclei

The left nucleus

$$\mathbb{N}_l(\mathbb{S}) := \{x \ : \ x \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall y, z \in \mathbb{S}\},$$

Nuclei

The left nucleus

$$\mathbb{N}_l(\mathbb{S}) := \{x \ : \ x \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall y, z \in \mathbb{S}\},$$

The middle nucleus

$$\mathbb{N}_m(\mathbb{S}) := \{y \ : \ y \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall x, z \in \mathbb{S}\},$$

The right nucleus

$$\mathbb{N}_r(\mathbb{S}) := \{z \ : \ z \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall x, y \in \mathbb{S}\}.$$

Nuclei

The left nucleus

$$\mathbb{N}_l(\mathbb{S}) := \{x \ : \ x \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall y, z \in \mathbb{S}\},$$

The middle nucleus

$$\mathbb{N}_m(\mathbb{S}) := \{y \ : \ y \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall x, z \in \mathbb{S}\},$$

The right nucleus

$$\mathbb{N}_r(\mathbb{S}) := \{z \ : \ z \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall x, y \in \mathbb{S}\}.$$

The center

$$Z(\mathbb{S}) := \{c \ : \ c \in \mathbb{N}_l(\mathbb{S}) \cap \mathbb{N}_m(\mathbb{S}) \cap \mathbb{N}_r(\mathbb{S}) \mid x \circ c = c \circ x, \forall x \in \mathbb{S}\}.$$

Nuclei

The left nucleus

$$\mathbb{N}_l(\mathbb{S}) := \{x \; : \; x \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \;\forall y, z \in \mathbb{S}\},$$

The middle nucleus

$$\mathbb{N}_m(\mathbb{S}) := \{y \; : \; y \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \;\forall x, z \in \mathbb{S}\},$$

The right nucleus

$$\mathbb{N}_r(\mathbb{S}) := \{z \; : \; z \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \;\forall x, y \in \mathbb{S}\}.$$

The center

$$Z(\mathbb{S}) := \{c \; : \; c \in \mathbb{N}_l(\mathbb{S}) \cap \mathbb{N}_m(\mathbb{S}) \cap \mathbb{N}_r(\mathbb{S}) \mid x \circ c = c \circ x, \forall x \in \mathbb{S}\}.$$

$\Rightarrow$ left vector space over the left nucleus $\mathbb{N}_l(\mathbb{S}) =: V_l(\mathbb{S})$
$\Rightarrow$ right vector space over the right nucleus $\mathbb{N}_r(\mathbb{S}) =: V_r(\mathbb{S})$

$$y^{L_x} = x \circ y \Rightarrow L_x \in End(V_r(\mathbb{S}))$$

$$y^{R_x} = y \circ x \Rightarrow R_x \in End(V_l(\mathbb{S}))$$

Action of $Sym(3)$ on the isotopism classes

Action of $Sym(3)$ on the isotopism classes

- If $\{e_1, \ldots, e_n\}$ is a basis for $\mathbb{S}$ over the center $Z(\mathbb{S})$, then the structure constants a_{ijk} are given by

$$e_i \circ e_j = \sum_{i=1}^{n} a_{ijk} e_k$$

Action of $Sym(3)$ on the isotopism classes

- If $\{e_1, \ldots, e_n\}$ is a basis for $\mathbb{S}$ over the center $Z(\mathbb{S})$, then the structure constants a_{ijk} are given by

$$e_i \circ e_j = \sum_{i=1}^{n} a_{ijk} e_k$$

- Permuting the indices of the a_{ijk} gives six semifields (Knuth 1965) $\Rightarrow$ six semifields $\mathbb{S}_1, \ldots, \mathbb{S}_6$

Action of $Sym(3)$ on the isotopism classes

- If $\{e_1, \ldots, e_n\}$ is a basis for $\mathbb{S}$ over the center $Z(\mathbb{S})$, then the structure constants a_{ijk} are given by

$$e_i \circ e_j = \sum_{i=1}^{n} a_{ijk} e_k$$

- Permuting the indices of the a_{ijk} gives six semifields (Knuth 1965) $\Rightarrow$ six semifields $\mathbb{S}_1, \ldots, \mathbb{S}_6$
- Knuth orbit $\mathcal{K}(\mathbb{S})$:= $\{[\mathbb{S}_1], \ldots, [\mathbb{S}_6]\}$

The Knuthorbit of a semifield $\mathbb{S}$

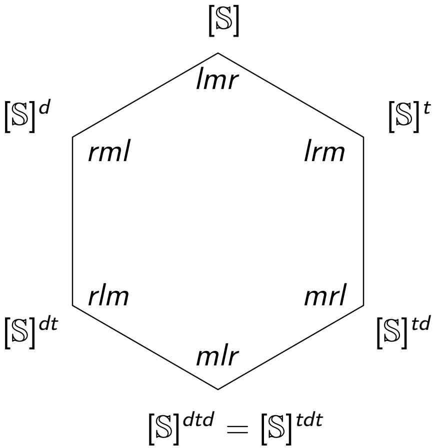


Figure: The nuclei are denoted by l, m, r

A GEOMETRIC APPROACH TO FINITE SEMIFIELDS

- Construction of examples
- Proving that these examples are "new"
- Extension of the Knuth orbit
- Classification results

1. General case
2. Two-dimensional case ($dim V_l(\mathbb{S}) = 2$)
3. Commutative semifields and symplectic semifields
4. Rank two commutative semifields (RTCS)

1. The general case

1. The general case

- A spread of $\mathrm{PG}(V)$ is a partition of the pointset by subspaces of the same dimension.

1. The general case

- A spread of $\mathrm{PG}(V)$ is a partition of the pointset by subspaces of the same dimension.
- A spread $\mathcal{D}$ is called Desarguesian if $\mathcal{D}$ is obtained by "field-reduction" from a projective space $\pi(D)$

1. The general case

- A spread of $\mathrm{PG}(V)$ is a partition of the pointset by subspaces of the same dimension.
- A spread $\mathcal{D}$ is called Desarguesian if $\mathcal{D}$ is obtained by "field-reduction" from a projective space $\pi(D)$
- If $\mathcal{D}$ is a spread of $\mathrm{PG}(V)$, and T is a subset of $\mathrm{PG}(V)$ then we define

$$B_{\mathcal{D}}(T) := \{S \in \mathcal{D} \ : \ S \cap T \neq \emptyset\}$$

1. The general case

- A spread of $\mathrm{PG}(V)$ is a partition of the pointset by subspaces of the same dimension.
- A spread $\mathcal{D}$ is called Desarguesian if $\mathcal{D}$ is obtained by "field-reduction" from a projective space $\pi(D)$
- If $\mathcal{D}$ is a spread of $\mathrm{PG}(V)$, and T is a subset of $\mathrm{PG}(V)$ then we define
$$B_{\mathcal{D}}(T) := \{S \in \mathcal{D} \ : \ S \cap T \neq \emptyset\}$$
- If T is a subspace, and $\mathcal{D}$ is a Desarguesian spread, then $B_{\mathcal{D}}(T) \hookrightarrow \pi(\mathcal{D})$ is called a linear set of $\pi(\mathcal{D})$.

1. The general case

- A spread of $\mathrm{PG}(V)$ is a partition of the pointset by subspaces of the same dimension.
- A spread $\mathcal{D}$ is called Desarguesian if $\mathcal{D}$ is obtained by "field-reduction" from a projective space $\pi(D)$
- If $\mathcal{D}$ is a spread of $\mathrm{PG}(V)$, and T is a subset of $\mathrm{PG}(V)$ then we define
$$B_{\mathcal{D}}(T) := \{S \in \mathcal{D} \ : \ S \cap T \neq \emptyset\}$$
- If T is a subspace, and $\mathcal{D}$ is a Desarguesian spread, then $B_{\mathcal{D}}(T) \hookrightarrow \pi(\mathcal{D})$ is called a linear set of $\pi(\mathcal{D})$.
- If T has dimension d, then $B_{\mathcal{D}}(T)$ is a linear set of rank $d+1$

1. The general case: linear sets from a semifield $\mathbb{S}$

1. The general case: linear sets from a semifield $\mathbb{S}$

- The set $\{R_x \ : \ x \in \mathbb{S}\} \subset End(V_l(\mathbb{S}))$ is an $\mathbb{F}_q$-vector space of dimension n.

1. The general case: linear sets from a semifield $\mathbb{S}$

- The set $\{R_x \ : \ x \in \mathbb{S}\} \subset End(V_l(\mathbb{S}))$ is an $\mathbb{F}_q$-vector space of dimension n.

  $\Rightarrow$ $\mathbb{F}_q$-linear set $L(\mathbb{S})$ in $\mathrm{PG}(End(V_l(\mathbb{S}))) = \mathrm{PG}(l^2-1, q^{n/l})$ of rank n.

1. The general case: linear sets from a semifield $\mathbb{S}$

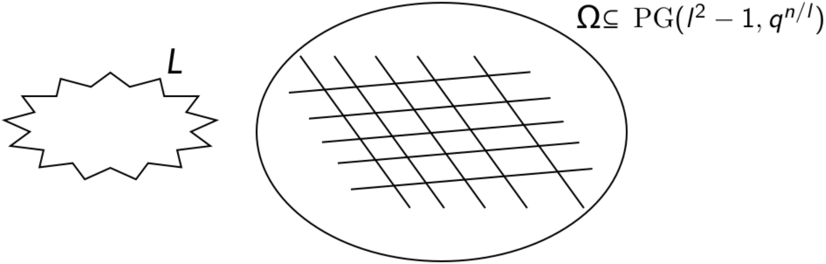
- The set $\{R_x \ : \ x \in \mathbb{S}\} \subset End(V_l(\mathbb{S}))$ is an $\mathbb{F}_q$-vector space of dimension n.

  $\Rightarrow$ $\mathbb{F}_q$-linear set $L(\mathbb{S})$ in $\mathrm{PG}(End(V_l(\mathbb{S}))) = \mathrm{PG}(l^2 - 1, q^{n/l})$ of rank n.
- Since $\mathbb{S}$ has no zero divisors, R_x is non-singular and hence $L(\mathbb{S})$ is disjoint from the $(l-2)$nd secant variety of the Segre variety $\mathcal{S}_{l,l}(q^{n/l})$.

1. The general case: linear sets from a semifield $\mathbb{S}$

- The set $\{R_x \ : \ x \in \mathbb{S}\} \subset End(V_l(\mathbb{S}))$ is an $\mathbb{F}_q$-vector space of dimension n.

  $\Rightarrow$ $\mathbb{F}_q$-linear set $L(\mathbb{S})$ in $\mathrm{PG}(End(V_l(\mathbb{S}))) = \mathrm{PG}(l^2-1, q^{n/l})$ of rank n.
- Since $\mathbb{S}$ has no zero divisors, R_x is non-singular and hence $L(\mathbb{S})$ is disjoint from the $(l-2)$nd secant variety of the Segre variety $\mathcal{S}_{l,l}(q^{n/l})$.
- Denote this secant variety by Ω



1. The general case: isotopism $\rightarrow$ orbits in $PG(l^2 - 1, q^{n/l})$

1. The general case: isotopism $\rightarrow$ orbits in $PG(l^2-1, q^{n/l})$

- Let G denote the stabiliser of the two families of maximal subpaces on $\mathcal{S}_{l,l}(q^{n/l})$.

1. The general case: isotopism $\rightarrow$ orbits in $PG(l^2-1, q^{n/l})$

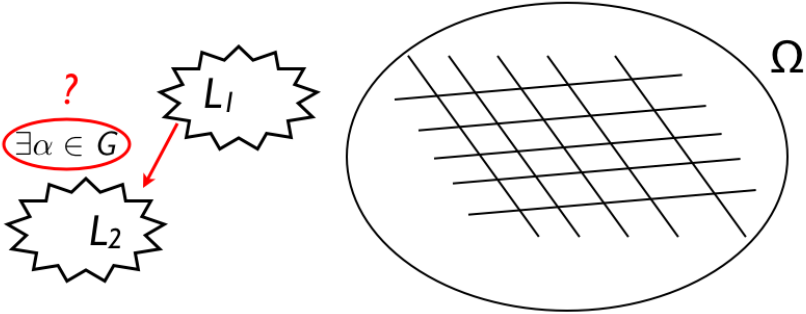
- Let G denote the stabiliser of the two families of maximal subpaces on $\mathcal{S}_{l,l}(q^{n/l})$.
- Let X denote the set of linear sets of rank n disjoint from Ω.

1. The general case: isotopism $\rightarrow$ orbits in $PG(l^2-1, q^{n/l})$

- Let G denote the stabiliser of the two families of maximal subpaces on $\mathcal{S}_{l,l}(q^{n/l})$.
- Let X denote the set of linear sets of rank n disjoint from Ω.

Theorem (ML2011)

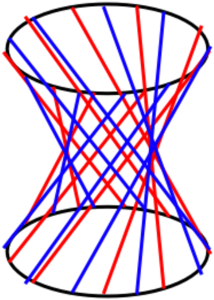
There is a one-to-one correspondence between the isotopism classes of semifields of order q^n, l-dimensional over their left nucleus and the orbits of G on the set X.



2. Rank two semifields (l=2) (2-dim over left nucleus)

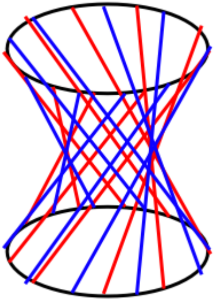
2. Rank two semifields (l=2) (2-dim over left nucleus)

- $L(\mathbb{S})$ is an $\mathbb{F}_q$-linear set in $\mathrm{PG}(3, q^{n/2})$ disjoint from a hyperbolic quadric



2. Rank two semifields (l=2) (2-dim over left nucleus)

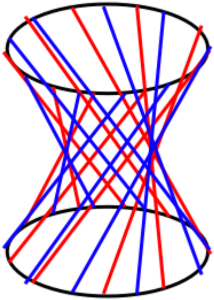
- $L(\mathbb{S})$ is an $\mathbb{F}_q$-linear set in $\mathrm{PG}(3, q^{n/2})$ disjoint from a hyperbolic quadric



- Classification for $n = 4$ (Cardinali - Polverino - Trombetti, 2006)

2. Rank two semifields (l=2) (2-dim over left nucleus)

- $L(\mathbb{S})$ is an $\mathbb{F}_q$-linear set in $\mathrm{PG}(3, q^{n/2})$ disjoint from a hyperbolic quadric



- Classification for $n = 4$ (Cardinali - Polverino - Trombetti, 2006)
- Towards a classification for $n = 6$ (Marino - Polverino - Trombetti)

2. Rank two semifields (l=2) (2-dim over left nucleus)

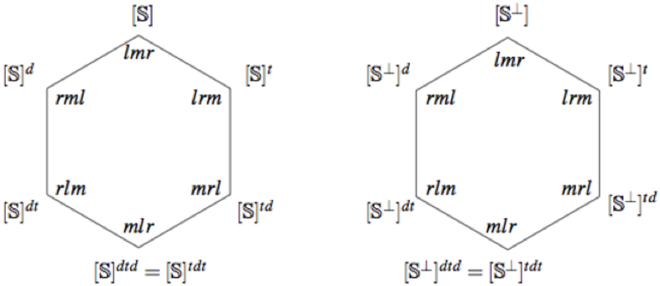
- Lot's of new examples (see Giuseppe's talk)

2. Rank two semifields (l=2) (2-dim over left nucleus)

- Lot's of new examples (see Giuseppe's talk)
- Extension of the Knuth orbit $\rightarrow$ translation dual

$$\mathbb{S} \mapsto \mathbb{S}^{\perp}$$

[Lunardon - Marino - Polverino - Trombetti 2008], special case of "switching" from [Ball - Ebert - ML 2007]



3. Symplectic semifields and commutative semifields

3. Symplectic semifields and commutative semifields

Theorem (Kantor 2003)

A pre–semifield $\mathbb{S}$ *is symplectic if and only if the pre–semifield* $\mathbb{S}^{dt}$ *is isotopic to a commutative semifield.*

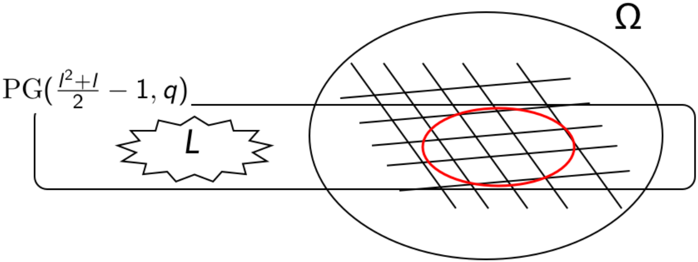
3. Symplectic semifields and commutative semifields

Theorem (Kantor 2003)

A pre–semifield $\mathbb{S}$ is symplectic if and only if the pre–semifield $\mathbb{S}^{dt}$ is isotopic to a commutative semifield.

Theorem (Lunardon-Marino-Polverino-Trombetti 2011)

$\mathbb{S}$ is symplectic $\iff$ $L(\mathbb{S})$ is contained in an $(\frac{l^2+l}{2}-1)$-dimensional subspace intersecting $\mathcal{S}_{l,l}(q^{n/l})$ in a Veronese variety $\mathcal{V}_l(q^{n/l})$



3. Symplectic semifields and commutative semifields

- Extension of the Knuth orbit if $l = 3 \rightarrow$ symplectic dual (using polarity in $\mathrm{PG}(5, q^{n/3})$ containing $\mathcal{V}_3(q^{n/3})$) [Lunardon, Marino, Polverino, Trombetti]

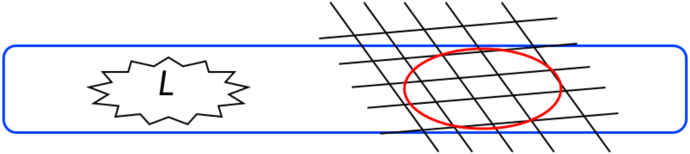
3. Symplectic semifields and commutative semifields

- Extension of the Knuth orbit if $l = 3 \rightarrow$ symplectic dual (using polarity in $\mathrm{PG}(5, q^{n/3})$ containing $\mathcal{V}_3(q^{n/3})$) [Lunardon, Marino, Polverino, Trombetti]
- New examples
- Perfect nonlinear functions, equiangular lines, MUBS, ...

4. Rank two commutative semifields (RTCS)

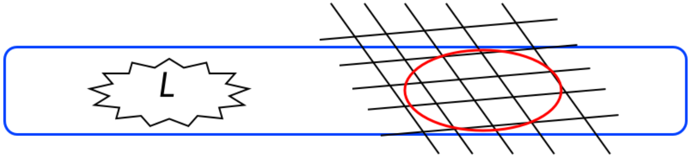
4. Rank two commutative semifields (RTCS)

- $L(\mathbb{S})$ is contained in a plane intersecting $Q^+(3, q^{n/2})$ in a conic



4. Rank two commutative semifields (RTCS)

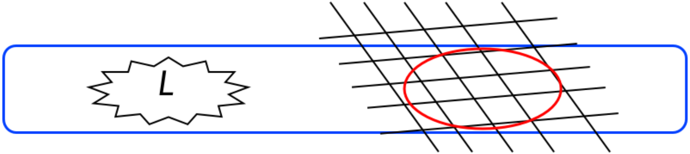
- $L(\mathbb{S})$ is contained in a plane intersecting $Q^+(3, q^{n/2})$ in a conic



- many links with other structures in finite geometry, e.g. flocks of a quadratic cone and translation ovoids of GQ, pseudo-ovoids ("eggs") and TGQ

4. Rank two commutative semifields (RTCS)

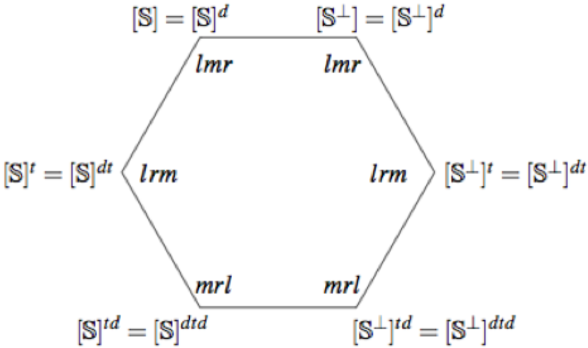
- $L(\mathbb{S})$ is contained in a plane intersecting $Q^+(3, q^{n/2})$ in a conic



- many links with other structures in finite geometry, e.g. flocks of a quadratic cone and translation ovoids of GQ, pseudo-ovoids ("eggs") and TGQ
- few examples known: field, Dickson (1906), Cohen-Ganley (1982), Penttila-Williams (1999)

4. Rank two commutative semifields (RTCS)

- Knuth-orbit [Ball - Brown 2004]



4. Rank two commutative semifields (RTCS)

- classification results

4. Rank two commutative semifields (RTCS)

- classification results

Theorem (Cohen - Ganley 1982)

For q even the only RTCS of order q^2 is the finite field $\mathbb{F}_{q^2}$.

4. Rank two commutative semifields (RTCS)

- classification results

Theorem (Cohen - Ganley 1982)

For q even the only RTCS of order q^2 is the finite field $\mathbb{F}_{q^2}$.

Theorem (Ball - Blokhuis - ML 2003, ML 2006)

Let $\mathbb{S}$ be an RTCS of order q^{2n}, q an odd prime power (p^{2n}, p an odd prime), with center $\mathbb{F}_q$. If $q \geq 4n^2 - 8n + 2$ ($p > 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$), then $\mathbb{S}$ is either a field or a RTCS of Dickson type.

GEOMETRIC CONSTRUCTION: BEL-configuration

BEL-configuration $(\mathcal{D}, U, W)$ in $\Sigma := \mathrm{PG}(rn-1, q)$ $(2 \leq r)$

GEOMETRIC CONSTRUCTION: BEL-configuration

BEL-configuration $(\mathcal{D}, U, W)$ in $\Sigma := \mathrm{PG}(rn-1, q)$ $(2 \leq r)$

- $\mathcal{D}$ a Desarguesian $(n-1)$-spread of Σ

GEOMETRIC CONSTRUCTION: BEL-configuration

BEL-configuration $(\mathcal{D}, U, W)$ in $\Sigma := \mathrm{PG}(rn-1, q)$ $(2 \leq r)$

- $\mathcal{D}$ a Desarguesian $(n-1)$-spread of Σ
- Let

$$\begin{cases} U \subset \Sigma \text{ , } \dim(U) = n-1 \\ W \subset \Sigma \text{ , } \dim(W) = rn-n-1 \end{cases}$$

GEOMETRIC CONSTRUCTION: BEL-configuration

BEL-configuration $(\mathcal{D}, U, W)$ in $\Sigma := \mathrm{PG}(rn-1, q)$ $(2 \leq r)$

- $\mathcal{D}$ a Desarguesian $(n-1)$-spread of Σ
- Let

$$\begin{cases} U \subset \Sigma \,, \dim(U) = n-1 \\ W \subset \Sigma \,, \dim(W) = rn-n-1 \end{cases}$$

such that no element of $\mathcal{D}$ intersects both U and W

GEOMETRIC CONSTRUCTION: BEL-configuration

BEL-configuration $(\mathcal{D}, U, W)$ in $\Sigma := \mathrm{PG}(rn-1, q)$ $(2 \leq r)$

- $\mathcal{D}$ a Desarguesian $(n-1)$-spread of Σ
- Let

$$\begin{cases} U \subset \Sigma \text{ , } \dim(U) = n-1 \\ W \subset \Sigma \text{ , } \dim(W) = rn-n-1 \end{cases}$$

such that no element of $\mathcal{D}$ intersects both U and W

Theorem (Ball-Ebert-ML 2007)

BEL-configuration $(\mathcal{D}, U, W)$ *gives rise to a finite semifield* $\mathbb{S}(\mathcal{D}, U, W)$ *of order* q^n *whose center contains* $\mathbb{F}_q$*,*

GEOMETRIC CONSTRUCTION: BEL-configuration

BEL-configuration $(\mathcal{D}, U, W)$ in $\Sigma := \mathrm{PG}(rn-1, q)$ $(2 \leq r)$

- $\mathcal{D}$ a Desarguesian $(n-1)$-spread of Σ
- Let
$$\begin{cases} U \subset \Sigma \text{ , } \dim(U) = n-1 \\ W \subset \Sigma \text{ , } \dim(W) = rn-n-1 \end{cases}$$
such that no element of $\mathcal{D}$ intersects both U and W

Theorem (Ball-Ebert-ML 2007)

BEL-configuration $(\mathcal{D}, U, W)$ gives rise to a finite semifield $\mathbb{S}(\mathcal{D}, U, W)$ of order q^n whose center contains $\mathbb{F}_q$, and conversely, every such semifield can be constructed in this way.

BEL-construction

BEL-construction

- Embed $\Sigma \hookrightarrow \Gamma := \mathrm{PG}(rn+n-1, q)$,

BEL-construction

- Embed $\Sigma \hookrightarrow \Gamma := \mathrm{PG}(rn + n - 1, q)$,
- Extend $\mathcal{D}$ to Γ $(\rightarrow \overline{\mathcal{D}})$,

BEL-construction

- Embed $\Sigma \hookrightarrow \Gamma := \mathrm{PG}(rn + n - 1, q)$,
- Extend $\mathcal{D}$ to Γ ($\rightarrow \overline{\mathcal{D}}$),
- Choose an n-space A, with $A \cap \Sigma = U$,

BEL-construction

- Embed $\Sigma \hookrightarrow \Gamma := \mathrm{PG}(rn + n - 1, q)$,
- Extend $\mathcal{D}$ to Γ ($\to \overline{\mathcal{D}}$),
- Choose an n-space A, with $A \cap \Sigma = U$,
- Then $B(A)$ induces a spread $\mathcal{S}$ in the quotient geometry $\Gamma/W \cong \mathrm{PG}(2n - 1, q)$

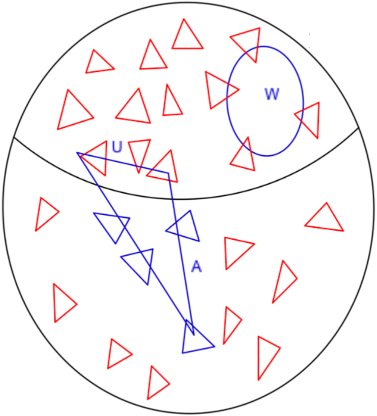
BEL-construction

- Embed $\Sigma \hookrightarrow \Gamma := \mathrm{PG}(rn + n - 1, q)$,
- Extend $\mathcal{D}$ to Γ $(\to \overline{\mathcal{D}})$,
- Choose an n-space A, with $A \cap \Sigma = U$,
- Then $B(A)$ induces a spread $\mathcal{S}$ in the quotient geometry $\Gamma/W \cong \mathrm{PG}(2n - 1, q)$
- Apply André-Bruck-Bose (spread $\mathcal{S} \to$ plane $\pi(\mathcal{S})$)

BEL-construction

- Embed $\Sigma \hookrightarrow \Gamma := \mathrm{PG}(rn + n - 1, q)$,
- Extend $\mathcal{D}$ to Γ ($\to \overline{\mathcal{D}}$),
- Choose an n-space A, with $A \cap \Sigma = U$,
- Then $B(A)$ induces a spread $\mathcal{S}$ in the quotient geometry $\Gamma/W \cong \mathrm{PG}(2n - 1, q)$
- Apply André-Bruck-Bose (spread $\mathcal{S} \to$ plane $\pi(\mathcal{S})$)
- plane $\pi(\mathcal{S}) \to \mathbb{S}(\mathcal{D}, U, W)$

BEL-construction



- If $r = 2$, U and W have the same dimension: $(\mathcal{D}, U, W) \to (\mathcal{D}, W, U)$: switching

TENSOR PRODUCT APPROACH

TENSOR PRODUCT APPROACH

Idea from a paper by R. Liebler (1981):

"*We have used [...] in hopes of making it clear that coordinates play no essential role in the study of class V planes. In fact, it is my view that coordinatization has played a role in the study of projective planes that is analogous to the role Artin [...] argues matrices have played in linear algebra.*"

TENSOR PRODUCT APPROACH

Consider $\bigotimes_{i \in I} V_i$ ($I = \{1, \ldots, m\}$, $m \geq 2$), with $\dim V_i = n_i$, and let $V_i^\vee$ denote the dual of V_i.

TENSOR PRODUCT APPROACH

Consider $\bigotimes_{i \in I} V_i$ ($I = \{1, \dots, m\}$, $m \geq 2$), with $\dim V_i = n_i$, and let $V_i^\vee$ denote the dual of V_i.

- fundamental tensors: $v_1 \otimes \dots \otimes v_r$, $v_i \in V_i$.

TENSOR PRODUCT APPROACH

Consider $\bigotimes_{i \in I} V_i$ ($I = \{1, \ldots, m\}$, $m \geq 2$), with $\dim V_i = n_i$, and let $V_i^{\vee}$ denote the dual of V_i.

- fundamental tensors: $v_1 \otimes \ldots \otimes v_r$, $v_i \in V_i$.
- contraction of fundamental tensor: for $v_i^{\vee} \in V_i^{\vee}$ define

$$v_i^{\vee}(u) := v_i^{\vee}(v_i)(v_1 \otimes \ldots \otimes v_{i-1} \otimes v_{i+1} \otimes \ldots \otimes v_m) \in \bigotimes_{j \in I, j \neq i} V_j.$$

TENSOR PRODUCT APPROACH

Consider $\bigotimes_{i \in I} V_i$ ($I = \{1, \dots, m\}$, $m \geq 2$), with $\dim V_i = n_i$, and let $V_i^\vee$ denote the dual of V_i.

- fundamental tensors: $v_1 \otimes \dots \otimes v_r$, $v_i \in V_i$.
- contraction of fundamental tensor: for $v_i^\vee \in V_i^\vee$ define

$$v_i^\vee(u) := v_i^\vee(v_i)(v_1 \otimes \dots \otimes v_{i-1} \otimes v_{i+1} \otimes \dots \otimes v_m) \in \bigotimes_{j \in I, j \neq i} V_j.$$

- extend this definition to contraction of a tensor

TENSOR PRODUCT APPROACH

Consider $\bigotimes_{i \in I} V_i$ ($I = \{1, \dots, m\}$, $m \geq 2$), with $\dim V_i = n_i$, and let $V_i^\vee$ denote the dual of V_i.

- fundamental tensors: $v_1 \otimes \dots \otimes v_r$, $v_i \in V_i$.
- contraction of fundamental tensor: for $v_i^\vee \in V_i^\vee$ define

$$v_i^\vee(u) := v_i^\vee(v_i)(v_1 \otimes \dots \otimes v_{i-1} \otimes v_{i+1} \otimes \dots \otimes v_m) \in \bigotimes_{j \in I, j \neq i} V_j.$$

- extend this definition to contraction of a tensor
- a nonzero vector of V_i is nonsingular

TENSOR PRODUCT APPROACH

Consider $\bigotimes_{i \in I} V_i$ ($I = \{1, \ldots, m\}$, $m \geq 2$), with $\dim V_i = n_i$, and let $V_i^\vee$ denote the dual of V_i.

- fundamental tensors: $v_1 \otimes \ldots \otimes v_r$, $v_i \in V_i$.
- contraction of fundamental tensor: for $v_i^\vee \in V_i^\vee$ define

$$v_i^\vee(u) := v_i^\vee(v_i)(v_1 \otimes \ldots \otimes v_{i-1} \otimes v_{i+1} \otimes \ldots \otimes v_m) \in \bigotimes_{j \in I, j \neq i} V_j.$$

- extend this definition to contraction of a tensor
- a nonzero vector of V_i is nonsingular
- $v \in \bigotimes_{i \in I} V_i$ is nonsingular if for $i \in I$ and every $v_i^\vee \in V_i^\vee$, the contraction $v_i^\vee(v)$ is nonsingular.

TENSOR PRODUCT APPROACH

Consider $\bigotimes_{i \in I} V_i$ ($I = \{1, \ldots, m\}$, $m \geq 2$), with $\dim V_i = n_i$, and let $V_i^\vee$ denote the dual of V_i.

- fundamental tensors: $v_1 \otimes \ldots \otimes v_r$, $v_i \in V_i$.
- contraction of fundamental tensor: for $v_i^\vee \in V_i^\vee$ define

$$v_i^\vee(u) := v_i^\vee(v_i)(v_1 \otimes \ldots \otimes v_{i-1} \otimes v_{i+1} \otimes \ldots \otimes v_m) \in \bigotimes_{j \in I, j \neq i} V_j.$$

- extend this definition to contraction of a tensor
- a nonzero vector of V_i is nonsingular
- $v \in \bigotimes_{i \in I} V_i$ is nonsingular if for $i \in I$ and every $v_i^\vee \in V_i^\vee$, the contraction $v_i^\vee(v)$ is nonsingular.
- the rank of a tensor T is the minimum number of fundamentals needed to generate T

Nonsingular tensors and semifields

Semifield $(\mathbb{S}, \circ) \to T_{\mathbb{S}} \in V^{\vee} \otimes V^{\vee} \otimes V$ with $V = \mathbb{F}_q^n$

Nonsingular tensors and semifields

Semifield $(\mathbb{S}, \circ) \to {\color{blue} T_{\mathbb{S}}} \in V^\vee \otimes V^\vee \otimes V$ with $V = \mathbb{F}_q^n$

$$\begin{tikzcd} V \times V \arrow[rr, "x \circ y"] \arrow[dr] & & V \\ & V \otimes V \arrow[ur, "h_{\mathbb{S}} \in \mathrm{Hom}_{\mathbb{F}}(V \otimes V, V)"'] & \end{tikzcd}$$

Nonsingular tensors and semifields

Semifield $(\mathbb{S}, \circ) \to T_{\mathbb{S}} \in V^{\vee} \otimes V^{\vee} \otimes V$ with $V = \mathbb{F}_q^n$

$$\begin{tikzcd} V \times V \arrow[rr, "x \circ y"] \arrow[dr] & & V \\ & V \otimes V \arrow[ur, "h_{\mathbb{S}} \in \mathrm{Hom}_{\mathbb{F}}(V \otimes V, V)"'] & \end{tikzcd}$$

$T_{\mathbb{S}} = \varphi^{-1}(h_{\mathbb{S}})$, where φ is defined by

$$\varphi : V^{\vee} \otimes V^{\vee} \otimes V \to \mathrm{Hom}_{\mathbb{F}}(V \otimes V, V)$$

$$(v_1 \otimes v_2)(u^{\vee} \otimes v^{\vee} \otimes w)^{\varphi} := u^{\vee}(v_1)v^{\vee}(v_2)w.$$

Nonsingular tensors and semifields

For convience, denote $V_1 = V_2 = V^\vee$ and $V_3 = V$

Nonsingular tensors and semifields

For convience, denote $V_1 = V_2 = V^\vee$ and $V_3 = V$

Theorem

(i) *The tensor* $T_{\mathbb{S}} \in V_1 \otimes V_2 \otimes V_3$ *is nonsingular.*
(ii) *To every nonsingular tensor* $T \in V_1 \otimes V_2 \otimes V_3$ *there corresponds a presemifield* $\mathbb{S}$ *for which* $T = T_{\mathbb{S}}$*.*
(iii) *The map* $\mathbb{S} \mapsto T_{\mathbb{S}}$ *is injective.*

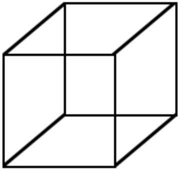
Nonsingular tensors and semifields

For convience, denote $V_1 = V_2 = V^\vee$ and $V_3 = V$

Theorem

(i) *The tensor $T_{\mathbb{S}} \in V_1 \otimes V_2 \otimes V_3$ is nonsingular.*
(ii) *To every nonsingular tensor $T \in V_1 \otimes V_2 \otimes V_3$ there corresponds a presemifield $\mathbb{S}$ for which $T = T_{\mathbb{S}}$.*
(iii) *The map $\mathbb{S} \mapsto T_{\mathbb{S}}$ is injective.*

(Knuth 1965) *With bases of V_i $\rightarrow$ cube of structure constants a_{ijk}*



In projective space

- $(\mathbb{S}, \circ) \to p_{\mathbb{S}} := \langle T_{\mathbb{S}} \rangle \in \mathrm{PG}(V_1 \otimes V_2 \otimes V_3)$
- $p_{\mathbb{S}_1} = p_{\mathbb{S}_2}$ implies $[\mathbb{S}_1] = [\mathbb{S}_2]$.

In projective space

- $(\mathbb{S}, \circ) \to p_{\mathbb{S}} := \langle T_{\mathbb{S}} \rangle \in \mathrm{PG}(V_1 \otimes V_2 \otimes V_3)$
- $p_{\mathbb{S}_1} = p_{\mathbb{S}_2}$ implies $[\mathbb{S}_1] = [\mathbb{S}_2]$.

Theorem

(i) $[\mathbb{S}_1] = [\mathbb{S}_2] \iff p^{\mathcal{G}}_{\mathbb{S}_1} = p^{\mathcal{G}}_{\mathbb{S}_2}$, *where* $\mathcal{G}$ *is the collineation group that fixes the three families of maximal subspaces of the Segre variety* $S_{n,n,n}(q)$*;*

In projective space

- $(\mathbb{S}, \circ) \to p_{\mathbb{S}} := \langle T_{\mathbb{S}} \rangle \in \mathrm{PG}(V_1 \otimes V_2 \otimes V_3)$
- $p_{\mathbb{S}_1} = p_{\mathbb{S}_2}$ implies $[\mathbb{S}_1] = [\mathbb{S}_2]$.

Theorem

(i) $[\mathbb{S}_1] = [\mathbb{S}_2] \iff p^{\mathcal{G}}_{\mathbb{S}_1} = p^{\mathcal{G}}_{\mathbb{S}_2}$*, where* $\mathcal{G}$ *is the collineation group that fixes the three families of maximal subspaces of the Segre variety* $S_{n,n,n}(q)$*;*
(ii) $\mathcal{K}(\mathbb{S}_1) = \mathcal{K}(\mathbb{S}_2) \iff p^{\mathcal{H}}_{\mathbb{S}_1} = p^{\mathcal{H}}_{\mathbb{S}_2}$*, where* $\mathcal{H}$ *is the stabiliser of the Segre variety* $S_{n,n,n}(q)$*.*

The tensor rank $\mathrm{trk}(\mathbb{S})$ of a semifield $\mathbb{S}$

The tensor rank $\mathrm{trk}(\mathbb{S})$ of a semifield $\mathbb{S}$

- The tensor rank of $\mathbb{S}$ is the rank of $T_{\mathbb{S}}$

The tensor rank $\mathrm{trk}(\mathbb{S})$ of a semifield $\mathbb{S}$

- The tensor rank of $\mathbb{S}$ is the rank of $T_{\mathbb{S}}$
- Geometrically: $\mathrm{trk}(\mathbb{S}) :=$ minimum number of points $s_1, \ldots, s_k \in S_{n,n,n}(q)$ such that $p_{\mathbb{S}} \subset \langle s_1, \ldots, s_k \rangle$.

The tensor rank $\mathrm{trk}(\mathbb{S})$ of a semifield $\mathbb{S}$

- The tensor rank of $\mathbb{S}$ is the rank of $T_{\mathbb{S}}$
- Geometrically: $\mathrm{trk}(\mathbb{S}) :=$ minimum number of points $s_1, \ldots, s_k \in S_{n,n,n}(q)$ such that $p_{\mathbb{S}} \subset \langle s_1, \ldots, s_k \rangle$.
- The $\mathrm{trk}(\mathbb{S})$ is an invariant of the isotopism class

Final remarks

Final remarks

- Geometric approach has contributed a lot in semifield theory.

Final remarks

- Geometric approach has contributed a lot in semifield theory.
- Still lot's of interesting questions unsolved (RTCS, symplectic, switching, ...)

Final remarks

- Geometric approach has contributed a lot in semifield theory.
- Still lot's of interesting questions unsolved (RTCS, symplectic, switching, ...)
- The power of this coordinate-free representation is demonstrated in [Liebler1981]

Final remarks

- Geometric approach has contributed a lot in semifield theory.
- Still lot's of interesting questions unsolved (RTCS, symplectic, switching, ...)
- The power of this coordinate-free representation is demonstrated in [Liebler1981]
- The tensor approach gives us a nice representation of the Knuth orbit, which we didn't see before.

Final remarks

- Geometric approach has contributed a lot in semifield theory.
- Still lot's of interesting questions unsolved (RTCS, symplectic, switching, ...)
- The power of this coordinate-free representation is demonstrated in [Liebler1981]
- The tensor approach gives us a nice representation of the Knuth orbit, which we didn't see before.
- We can construct the 6 subspaces skew from the secant variety Ω starting from a nonsingular tensor point.

Final remarks

- Geometric approach has contributed a lot in semifield theory.
- Still lot's of interesting questions unsolved (RTCS, symplectic, switching, ...)
- The power of this coordinate-free representation is demonstrated in [Liebler1981]
- The tensor approach gives us a nice representation of the Knuth orbit, which we didn't see before.
- We can construct the 6 subspaces skew from the secant variety Ω starting from a nonsingular tensor point.
- The properties of a nonsingular tensor gives us a geometric characterisation of the points of $\mathrm{PG}(n^3-1,q)$ that correspond to semifields.

Final remarks

- Geometric approach has contributed a lot in semifield theory.
- Still lot's of interesting questions unsolved (RTCS, symplectic, switching, ...)
- The power of this coordinate-free representation is demonstrated in [Liebler1981]
- The tensor approach gives us a nice representation of the Knuth orbit, which we didn't see before.
- We can construct the 6 subspaces skew from the secant variety Ω starting from a nonsingular tensor point.
- The properties of a nonsingular tensor gives us a geometric characterisation of the points of $\mathrm{PG}(n^3-1, q)$ that correspond to semifields.
- The tensor rank of a semifield is a measure for the complexity of the semifield multiplication.

Final remarks

- Geometric approach has contributed a lot in semifield theory.
- Still lot's of interesting questions unsolved (RTCS, symplectic, switching, ...)
- The power of this coordinate-free representation is demonstrated in [Liebler1981]
- The tensor approach gives us a nice representation of the Knuth orbit, which we didn't see before.
- We can construct the 6 subspaces skew from the secant variety Ω starting from a nonsingular tensor point.
- The properties of a nonsingular tensor gives us a geometric characterisation of the points of $\mathrm{PG}(n^3-1,q)$ that correspond to semifields.
- The tensor rank of a semifield is a measure for the complexity of the semifield multiplication.
- Thank you for your attention!