Semifields from skew polynomial rings

Michel Lavrauw

Università di Padova

Diamant Symposium
Heeze, May 26-27, 2011

(joint work with John Sheekey)

Research supported by the Research Foundation – Flanders (FWO)

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)

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 $\mathbb{F}_{q^k}$.
$\mathbb{S}_D$ is commutative, but not associative.

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 $\mathbb{F}_{q^k}$.
  $\mathbb{S}_D$ 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.

Semifields and Galois geometry

[ML - O. Polverino: Finite semifields. Chapter 6 in *Current research topics in Galois Geometry* Nova Academic Publishers (Editors J. De Beule and L. Storme)]

Semifields and Galois geometry

[ML - O. Polverino: Finite semifields. Chapter 6 in *Current research topics in Galois Geometry* Nova Academic Publishers (Editors J. De Beule and L. Storme)]

- Coordinatisation of projective planes (PTR's)
  $\longrightarrow$ semifield planes

Semifields and Galois geometry

[ML - O. Polverino: Finite semifields. Chapter 6 in *Current research topics in Galois Geometry* Nova Academic Publishers (Editors J. De Beule and L. Storme)]

- Coordinatisation of projective planes (PTR's)
  $\longrightarrow$ semifield planes
- Spreads

Semifields and Galois geometry

[ML - O. Polverino: Finite semifields. Chapter 6 in *Current research topics in Galois Geometry* Nova Academic Publishers (Editors J. De Beule and L. Storme)]

- Coordinatisation of projective planes (PTR's)
  $\longrightarrow$ semifield planes
- Spreads
- Ovoids of generalized quadrangles

Semifields and Galois geometry

[ML - O. Polverino: Finite semifields. Chapter 6 in *Current research topics in Galois Geometry* Nova Academic Publishers (Editors J. De Beule and L. Storme)]

- Coordinatisation of projective planes (PTR's)
  $\longrightarrow$ semifield planes
- Spreads
- Ovoids of generalized quadrangles
- Translation generalized quadrangles

Semifields and Galois geometry

[ML - O. Polverino: Finite semifields. Chapter 6 in *Current research topics in Galois Geometry* Nova Academic Publishers (Editors J. De Beule and L. Storme)]

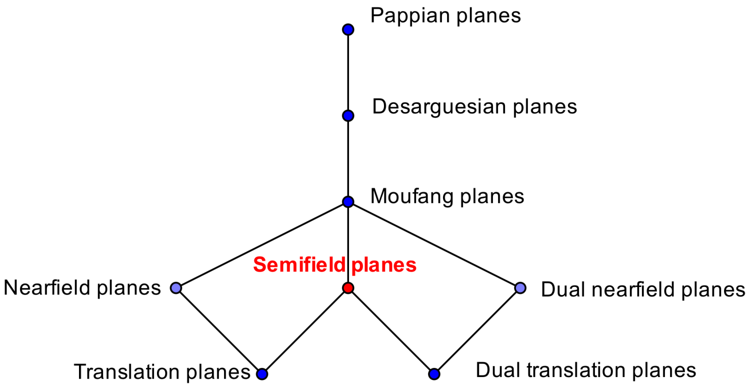
- Coordinatisation of projective planes (PTR's)
  $\longrightarrow$ semifield planes
- Spreads
- Ovoids of generalized quadrangles
- Translation generalized quadrangles
- Blocking sets

Semifields and Galois geometry

[ML - O. Polverino: Finite semifields. Chapter 6 in *Current research topics in Galois Geometry* Nova Academic Publishers (Editors J. De Beule and L. Storme)]

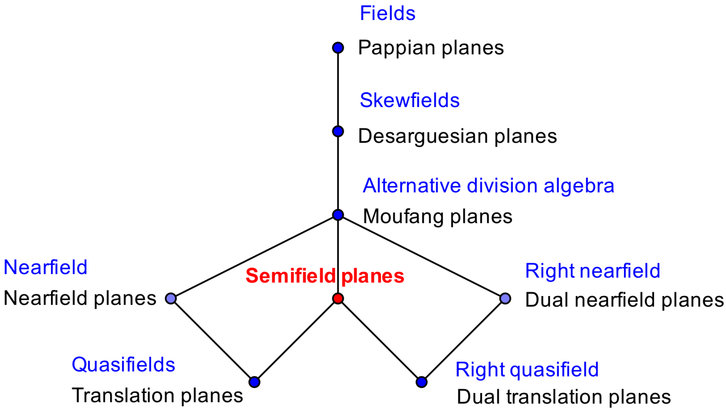
- Coordinatisation of projective planes (PTR's) $\longrightarrow$ semifield planes
- Spreads
- Ovoids of generalized quadrangles
- Translation generalized quadrangles
- Blocking sets
- ...

Types of translation planes and their PTR's



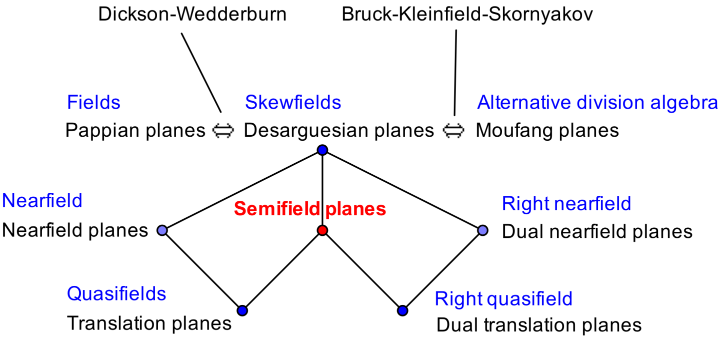
[Hughes - Piper, Projective Planes, Springer, 1973]

Types of translation planes and their PTR's



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

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 $[\mathbb{S}]$

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 $\{e_1, \dots, e_n\}$ 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 $\mathbb{S}_1, \dots, \mathbb{S}_6$
- Knuth orbit:$=\{[\mathbb{S}_1], \dots, [\mathbb{S}_6]\}$

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

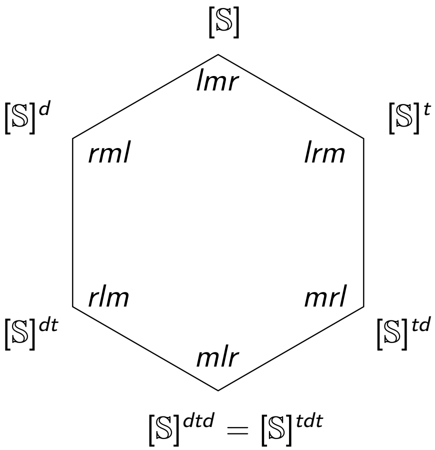


Figure: The nuclei are denoted by l, m, r

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

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

Cyclic semifields

Cyclic semifields

- Construction by Jha and Johnson (1989) using an irreducible semilinear map.

Cyclic semifields

- Construction by Jha and Johnson (1989) using an irreducible semilinear map.
- Let $T \in \Gamma\mathrm{L}(\mathbb{F}_{q^n}^d)$ be irreducible and for $x, y \in \mathbb{F}_{q^n}^d$ define

$$y \circ x := y \left(\sum_{i=0}^{d-1} T^i x_i \right), \text{ where } x = (x_0, \ldots, x_{d-1}).$$

Then this defines a semifield $\mathbb{S}_T$ of size q^{nd}.

Cyclic semifields

- Construction by Jha and Johnson (1989) using an irreducible semilinear map.
- Let $T \in \Gamma\mathrm{L}(\mathbb{F}_{q^n}^d)$ be irreducible and for $x, y \in \mathbb{F}_{q^n}^d$ define

$$y \circ x := y\left(\sum_{i=0}^{d-1} T^i x_i\right), \text{ where } x = (x_0, \ldots, x_{d-1}).$$

  Then this defines a semifield $\mathbb{S}_T$ of size q^{nd}.
- This construction has been generalized by Johnson - Marino - Polverino - Trombetti (2008)

Cyclic semifields

- Construction by Jha and Johnson (1989) using an irreducible semilinear map.
- Let $T \in \Gamma\mathrm{L}(\mathbb{F}_{q^n}^d)$ be irreducible and for $x, y \in \mathbb{F}_{q^n}^d$ define

$$y \circ x := y\left(\sum_{i=0}^{d-1} T^i x_i\right), \text{ where } x = (x_0, \ldots, x_{d-1}).$$

  Then this defines a semifield $\mathbb{S}_T$ of size q^{nd}.
- This construction has been generalized by Johnson - Marino - Polverino - Trombetti (2008)
- Kantor - Liebler (2008): The number of isotopism classes of semifields $\mathbb{S}_T$ obtained from this construction is at most $q^d - 1$.
- Improved by Dempwolff (2011): $N(q, d)$

In this talk

1. Determine the nuclei of $\mathbb{S}_T$
2. Prove and improve the upper bound for the number of isotopism classes

Method: Skew polynomial rings

For $\sigma \in Aut(\mathbb{F})$, the skew polynomial ring $R := \mathbb{F}[t, \sigma]$ is the set

$$\{a_0 + a_1 t + \ldots + a_r t^r \;:\; a_i \in \mathbb{F}, r \in \mathbb{N}\}$$

with termwise addition and multiplication defined by

$$t^i a = a^{\sigma^i} t, \;\forall a \in \mathbb{F}$$

[1933] Oystein Ore, *Theory of Non-Commutative Polynomials*

Properties of skew polynomial rings

Properties:

Properties of skew polynomial rings

Properties:

- multiplication is associative, distributive, but not commutative,

Properties of skew polynomial rings

Properties:

- multiplication is associative, distributive, but not commutative,
- left- and right-Euclidean,
  $\Rightarrow$ left- and right-principal ideal domain,

Properties of skew polynomial rings

Properties:

- multiplication is associative, distributive, but not commutative,
- left- and right-Euclidean,
  $\Rightarrow$ left- and right-principal ideal domain,
- NOT unique factorisation domain,

Properties of skew polynomial rings

Properties:

- multiplication is associative, distributive, but not commutative,
- left- and right-Euclidean,
  $\Rightarrow$ left- and right-principal ideal domain,
- NOT unique factorisation domain,
- link with linearised polynomials
  (multiplication $\leftrightarrow$ composition),

Properties of skew polynomial rings

Properties:

- multiplication is associative, distributive, but not commutative,
- left- and right-Euclidean,
  $\Rightarrow$ left- and right-principal ideal domain,
- NOT unique factorisation domain,
- link with linearised polynomials
  (multiplication $\leftrightarrow$ composition),

Conventions:

1. we work with right divisors, unless otherwise stated,
2. the left ideal $R.f$ is denoted by $\langle f \rangle$.

Properties of the skew polynomial ring $\mathbb{F}_{q^n}[t, \sigma]$

Let $\mathbb{F} = \mathbb{F}_{q^n}$ and $\sigma \;:\; \mathbb{F}_{q^n} \to \mathbb{F}_{q^n} \;:\; a \mapsto a^q$

Properties of the skew polynomial ring $\mathbb{F}_{q^n}[t, \sigma]$

Let $\mathbb{F} = \mathbb{F}_{q^n}$ and $\sigma \ : \ \mathbb{F}_{q^n} \to \mathbb{F}_{q^n} \ : \ a \mapsto a^q$

- $Z :=$ the centre of $\mathbb{F}_{q^n}[t, \sigma]$ is $\mathbb{F}_q[t^n, \sigma] \cong \mathbb{F}_q[X]$

Properties of the skew polynomial ring $\mathbb{F}_{q^n}[t, \sigma]$

Let $\mathbb{F} = \mathbb{F}_{q^n}$ and $\sigma : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n} : a \mapsto a^q$

- $Z :=$ the centre of $\mathbb{F}_{q^n}[t, \sigma]$ is $\mathbb{F}_q[t^n, \sigma] \cong \mathbb{F}_q[X]$
- the two sided ideals in R are $\langle f \cdot t^s \rangle$ where $f \in Z$

Properties of the skew polynomial ring $\mathbb{F}_{q^n}[t, \sigma]$

Let $\mathbb{F} = \mathbb{F}_{q^n}$ and $\sigma \ : \ \mathbb{F}_{q^n} \to \mathbb{F}_{q^n} \ : \ a \mapsto a^q$

- $Z :=$ the centre of $\mathbb{F}_{q^n}[t, \sigma]$ is $\mathbb{F}_q[t^n, \sigma] \cong \mathbb{F}_q[X]$
- the two sided ideals in R are $\langle f \cdot t^s \rangle$ where $f \in Z$
- a polynomial $f \in R$ is called irreducible if f cannot be written as $f = gh$ with $deg(h) < deg(f)$ and $deg(g) < deg(f)$

Properties of the skew polynomial ring $\mathbb{F}_{q^n}[t, \sigma]$

Let $\mathbb{F} = \mathbb{F}_{q^n}$ and $\sigma \ : \ \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n} \ : \ a \mapsto a^q$

- $Z :=$ the centre of $\mathbb{F}_{q^n}[t, \sigma]$ is $\mathbb{F}_q[t^n, \sigma] \cong \mathbb{F}_q[X]$
- the two sided ideals in R are $\langle f \cdot t^s \rangle$ where $f \in Z$
- a polynomial $f \in R$ is called irreducible if f cannot be written as $f = gh$ with $deg(h) < deg(f)$ and $deg(g) < deg(f)$
- given f and g, the concepts of least common left multiple ($lclm(f, g)$) and greatest common right divisor ($gcrd(f, g)$) are well defined.

Semifields from skew polynomial rings

Let f be an irreducible polynomial of degree d in $\mathbb{F}_{q^n}[t,\sigma]$, and define a multiplication $\circ$ on the set of polynomials of degree less than d by

$$x \circ y := xy \mod f$$

Semifields from skew polynomial rings

Let f be an irreducible polynomial of degree d in $\mathbb{F}_{q^n}[t, \sigma]$, and define a multiplication $\circ$ on the set of polynomials of degree less than d by

$$x \circ y := xy \mod f$$

Theorem

The multiplication $\circ$ defines a semifield $\mathbb{S}_f := \mathbb{F}_{q^n}[t, \sigma]/\langle f \rangle$

[1932] Oystein Ore, *Formale Theorie der linearen Differentialgleichungen II*

[1934] Nathan Jacobson, *Non-Commutative Polynomials and Cyclic Algebras*

Semifields from skew polynomial rings

Proof.

(S3) Let $x, y \in \mathbb{S}_f$ and suppose $x \circ y = 0$ in $\mathbb{S}_f$. This means $\exists h \in \mathbb{F}_{q^n}[t, \sigma]$, s.t. $xy = hf$ in $\mathbb{F}_{q^n}[t, \sigma]$.

Semifields from skew polynomial rings

Proof.

(S3) Let $x, y \in \mathbb{S}_f$ and suppose $x \circ y = 0$ in $\mathbb{S}_f$. This means $\exists h \in \mathbb{F}_{q^n}[t,\sigma]$, s.t. $xy = hf$ in $\mathbb{F}_{q^n}[t,\sigma]$.

Theorem (Ore 1933)

If $f \in \mathbb{F}[t,\sigma]$ factors completely as

$$f = f_1 f_2 \dots f_k = g_1 g_2 \dots g_l,$$

where f_i and g_i are irreducible, then $k = l$ and there exists a permutation φ, s.t. $deg\ f_i = deg\ g_{\varphi(i)}$.

Semifields from skew polynomial rings

Proof.

(S3) Let $x, y \in \mathbb{S}_f$ and suppose $x \circ y = 0$ in $\mathbb{S}_f$. This means $\exists h \in \mathbb{F}_{q^n}[t, \sigma]$, s.t. $xy = hf$ in $\mathbb{F}_{q^n}[t, \sigma]$.

Theorem (Ore 1933)

If $f \in \mathbb{F}[t, \sigma]$ factors completely as

$$f = f_1 f_2 \dots f_k = g_1 g_2 \dots g_l,$$

where f_i and g_i are irreducible, then $k = l$ and there exists a permutation φ, s.t. $deg\ f_i = deg\ g_{\varphi(i)}$.

Proof continued $xy = hf$ in $\mathbb{F}_{q^n}[t, \sigma]$

Since f is irreducible of degree d, there must be a factor of x or of y that has degree d. Since both x and y have degree less than d, it follows that x or y must be 0. $\square$

Theorem

Each $\mathbb{S}_T$ is isotopic to some $\mathbb{S}_f$.

Theorem

Each $\mathbb{S}_T$ is isotopic to some $\mathbb{S}_f$.

Proof: Consider a basis $v, Tv, T^2v, \ldots, T^{d-1}v$, and suppose that

$$T^d v = \sum_{i=0}^{d-1} f_i T^i v.$$

Define a $\phi \in \mathrm{GL}(n, q^n)$: $\phi(t^i) := T^i$, then

$$T\phi = \phi L_{t,f},$$

where $L_{t,f}$ is left multiplication in $\mathbb{S}_f$ by t with

$$f(t) = t^d - \sum_{i=0}^{d-1} f_i t^i.$$

Theorem

Each $\mathbb{S}_T$ is isotopic to some $\mathbb{S}_f$.

Proof: Consider a basis $v, Tv, T^2v, \ldots, T^{d-1}v$, and suppose that

$$T^d v = \sum_{i=0}^{d-1} f_i T^i v.$$

Define a $\phi \in \mathrm{GL}(n, q^n)$: $\phi(t^i) := T^i$, then

$$T\phi = \phi L_{t,f},$$

where $L_{t,f}$ is left multiplication in $\mathbb{S}_f$ by t with

$$f(t) = t^d - \sum_{i=0}^{d-1} f_i t^i.$$

Kantor - Liebler: conjugate semilinear transformations define isotopic semifields.

The nuclei of $\mathbb{S}_f$

Theorem

If f is irreducible of degree d in $\mathbb{F}_{q^n}[t, \sigma]$, then

$$(\#\mathbb{S}_f, \#\mathbb{N}_l(\mathbb{S}_f), \#\mathbb{N}_m(\mathbb{S}_f), \#\mathbb{N}_r(\mathbb{S}_f), \#Z(\mathbb{S}_f)) = (q^{nd}, q^n, q^n, q^d, q)$$

Proof:

If $ab = uf + v$ and $bc = wf + z$, then

$$(ab)c = a(bc) \iff ufc + vc = awf + az,$$

and hence

$$(a \circ b) \circ c = a \circ (b \circ c) \iff vc = az \; mod f$$

$$\iff vc = ufc + vc \; mod f \iff ufc \; mod f = 0.$$

$\Rightarrow \mathbb{N}_l(\mathbb{S}_f) = \mathbb{N}_m(\mathbb{S}_f) = \mathbb{F}_{q^n}$, and $\mathbb{N}_r(\mathbb{S}_f) = E(f)$ eigenring of f.

Counting isotopism classes

Theorem (Odoni 1999)

The number of monic irreducibles of degree d in $\mathbb{F}_{q^n}[t,\sigma]$ is equal to

$$N(q,d)\frac{q^{nd}-1}{q^d-1},$$

where $N(q,d)$ is the number of monic irreducibles of degree d in $\mathbb{F}_q[X]$, i.e.,

$$N(q,d) = \frac{1}{d}\sum_{s|d}\mu(s)q^{d/s}.$$

Isotopisms for semifields $\mathbb{S}_f$

Isotopisms for semifields $\mathbb{S}_f$

Put $\mathcal{R} := \mathbb{F}_{q^n}[t, \sigma]$

Isotopisms for semifields $\mathbb{S}_f$

Put $\mathcal{R} := \mathbb{F}_{q^n}[t, \sigma]$

Lemma

If $f, g \in \mathcal{R}$ are irreducible of degree d and $\exists u, v \in \mathcal{R}$ of degree $< d$, s.t. $gu = vf$, then $[\mathbb{S}_f] = [\mathbb{S}_g]$. An isotopism is given by (id, R_u, R_u), where R_u is right multiplication in $\mathbb{S}_f$.

Isotopisms for semifields $\mathbb{S}_f$

Put $\mathcal{R} := \mathbb{F}_{q^n}[t, \sigma]$

Lemma

If $f, g \in \mathcal{R}$ are irreducible of degree d and $\exists u, v \in \mathcal{R}$ of degree $< d$, s.t. $gu = vf$, then $[\mathbb{S}_f] = [\mathbb{S}_g]$. An isotopism is given by (id, R_u, R_u), where R_u is right multiplication in $\mathbb{S}_f$.

Proof.

We show that

$$x \circ_f y^{R_u} = (x \circ_g y)^{R_u}.$$

Isotopisms for semifields $\mathbb{S}_f$

Put $\mathcal{R} := \mathbb{F}_{q^n}[t,\sigma]$

Lemma

If $f, g \in \mathcal{R}$ are irreducible of degree d and $\exists u, v \in \mathcal{R}$ of degree $< d$, s.t. $gu = vf$, then $[\mathbb{S}_f] = [\mathbb{S}_g]$. An isotopism is given by (id, R_u, R_u), where R_u is right multiplication in $\mathbb{S}_f$.

Proof.

We show that

$$x \circ_f y^{R_u} = (x \circ_g y)^{R_u}.$$

LHS $= x \circ_f (y \circ_f u) = x \circ_f (yu - af)$, for some $a \in \mathcal{R}$

Isotopisms for semifields $\mathbb{S}_f$

Put $\mathcal{R} := \mathbb{F}_{q^n}[t, \sigma]$

Lemma

If $f, g \in \mathcal{R}$ are irreducible of degree d and $\exists u, v \in \mathcal{R}$ of degree $< d$, s.t. $gu = vf$, then $[\mathbb{S}_f] = [\mathbb{S}_g]$. An isotopism is given by (id, R_u, R_u), where R_u is right multiplication in $\mathbb{S}_f$.

Proof.

We show that

$$x \circ_f y^{R_u} = (x \circ_g y)^{R_u}.$$

LHS $= x \circ_f (y \circ_f u) = x \circ_f (yu - af)$, for some $a \in \mathcal{R}$
$= x(yu - af) \mod f = xyu - xaf \mod f = xyu \mod f.$

Isotopisms for semifields $\mathbb{S}_f$

Put $\mathcal{R} := \mathbb{F}_{q^n}[t, \sigma]$

Lemma

If $f, g \in \mathcal{R}$ are irreducible of degree d and $\exists u, v \in \mathcal{R}$ of degree $< d$, s.t. $gu = vf$, then $[\mathbb{S}_f] = [\mathbb{S}_g]$. An isotopism is given by (id, R_u, R_u), where R_u is right multiplication in $\mathbb{S}_f$.

Proof.

We show that

$$x \circ_f y^{R_u} = (x \circ_g y)^{R_u}.$$

LHS $= x \circ_f (y \circ_f u) = x \circ_f (yu - af)$, for some $a \in \mathcal{R}$
$= x(yu - af) \mod f = xyu - xaf \mod f = xyu \mod f$.

RHS $= (x \circ_g y) \circ_f u = (xy - bg) \circ_f u$, for some $b \in \mathcal{R}$

Isotopisms for semifields $\mathbb{S}_f$

Put $\mathcal{R} := \mathbb{F}_{q^n}[t, \sigma]$

Lemma

If $f, g \in \mathcal{R}$ are irreducible of degree d and $\exists u, v \in \mathcal{R}$ of degree $< d$, s.t. $gu = vf$, then $[\mathbb{S}_f] = [\mathbb{S}_g]$. An isotopism is given by (id, R_u, R_u), where R_u is right multiplication in $\mathbb{S}_f$.

Proof.

We show that

$$x \circ_f y^{R_u} = (x \circ_g y)^{R_u}.$$

LHS $= x \circ_f (y \circ_f u) = x \circ_f (yu - af)$, for some $a \in \mathcal{R}$
$= x(yu - af) \mod f = xyu - xaf \mod f = xyu \mod f$.

RHS $= (x \circ_g y) \circ_f u = (xy - bg) \circ_f u$, for some $b \in \mathcal{R}$
$= (xy - bg)u \mod f = xyu - bgu \mod f = xyu \mod f$. $\square$

More properties of the skew polynomial ring $\mathcal{R} = \mathbb{F}_{q^n}[t, \sigma]$

Define the minimal central left multiple of $f \in \mathcal{R}$ ($mzlm(f)$ as the monic $g \in Z(\mathcal{R})$ of minimal degree s.t. $f|g$.

More properties of the skew polynomial ring $\mathcal{R} = \mathbb{F}_{q^n}[t, \sigma]$

Define the minimal central left multiple of $f \in \mathcal{R}$ ($mzlm(f)$) as the monic $g \in Z(\mathcal{R})$ of minimal degree s.t. $f|g$.

Properties:

More properties of the skew polynomial ring $\mathcal{R} = \mathbb{F}_{q^n}[t, \sigma]$

Define the minimal central left multiple of $f \in \mathcal{R}$ ($mzlm(f)$) as the monic $g \in Z(\mathcal{R})$ of minimal degree s.t. $f|g$.

Properties:

- Since $Z(\mathcal{R}) = \mathbb{F}_q[t^n, \sigma] \cong \mathbb{F}_q[X]$ it follows that $mzlm(f) = F(t^n)$, for some $F \in \mathbb{F}_q[X]$.

More properties of the skew polynomial ring $\mathcal{R} = \mathbb{F}_{q^n}[t, \sigma]$

Define the minimal central left multiple of $f \in \mathcal{R}$ ($mzlm(f)$) as the monic $g \in Z(\mathcal{R})$ of minimal degree s.t. $f | g$.

Properties:

- Since $Z(\mathcal{R}) = \mathbb{F}_q[t^n, \sigma] \cong \mathbb{F}_q[X]$ it follows that $mzlm(f) = F(t^n)$, for some $F \in \mathbb{F}_q[X]$.

Moreover if $f \in \mathcal{R}$ is irreducible of degree d:

More properties of the skew polynomial ring $\mathcal{R} = \mathbb{F}_{q^n}[t, \sigma]$

Define the minimal central left multiple of $f \in \mathcal{R}$ ($mzlm(f)$ as the monic $g \in Z(\mathcal{R})$ of minimal degree s.t. $f|g$.

Properties:

- Since $Z(\mathcal{R}) = \mathbb{F}_q[t^n, \sigma] \cong \mathbb{F}_q[X]$ it follows that $mzlm(f) = F(t^n)$, for some $F \in \mathbb{F}_q[X]$.

Moreover if $f \in \mathcal{R}$ is irreducible of degree d:

- $mzlm(f)$ exists, is unique and has degree nd

More properties of the skew polynomial ring $\mathcal{R} = \mathbb{F}_{q^n}[t, \sigma]$

Define the minimal central left multiple of $f \in \mathcal{R}$ ($mzlm(f)$ as the monic $g \in Z(\mathcal{R})$ of minimal degree s.t. $f|g$.

Properties:

- Since $Z(\mathcal{R}) = \mathbb{F}_q[t^n, \sigma] \cong \mathbb{F}_q[X]$ it follows that $mzlm(f) = F(t^n)$, for some $F \in \mathbb{F}_q[X]$.

Moreover if $f \in \mathcal{R}$ is irreducible of degree d:

- $mzlm(f)$ exists, is unique and has degree nd
- if $mzlm(f) = F(t^n)$, then F is irreducible of degree d in $\mathbb{F}_q[X]$

More properties of the skew polynomial ring $\mathcal{R} = \mathbb{F}_{q^n}[t, \sigma]$

Define the minimal central left multiple of $f \in \mathcal{R}$ ($mzlm(f)$ as the monic $g \in Z(\mathcal{R})$ of minimal degree s.t. $f|g$.

Properties:

- Since $Z(\mathcal{R}) = \mathbb{F}_q[t^n, \sigma] \cong \mathbb{F}_q[X]$ it follows that $mzlm(f) = F(t^n)$, for some $F \in \mathbb{F}_q[X]$.

Moreover if $f \in \mathcal{R}$ is irreducible of degree d:

- $mzlm(f)$ exists, is unique and has degree nd
- if $mzlm(f) = F(t^n)$, then F is irreducible of degree d in $\mathbb{F}_q[X]$
- if F is irreducible of degree d in $\mathbb{F}_q[X]$, then any irreducible divisor of $F(t^n)$ in $\mathcal{R}$ has degree d

Isotopisms for semifields $\mathbb{S}_f$

Isotopisms for semifields $\mathbb{S}_f$

Lemma

If $f, g \in \mathcal{R}$ are irreducible of degree d then the following are equivalent

(i) $\exists u, v \in \mathcal{R}$ *of degree* $< d$, *s.t.* $gu = vf$

(ii) $mzlm(f) = mzlm(g)$.

Isotopisms for semifields $\mathbb{S}_f$

Lemma

If $f, g \in \mathcal{R}$ are irreducible of degree d then the following are equivalent
(i) $\exists u, v \in \mathcal{R}$ of degree $< d$, s.t. $gu = vf$
(ii) $mzlm(f) = mzlm(g)$.

Corollary

(i) If $f, g \in \mathcal{R}$ are irreducible and $mzlm(f) = mzlm(g)$, then $[\mathbb{S}_f] = [\mathbb{S}_g]$
(ii) The number of isotopism classes of semifields $\mathbb{S}_f$ with $f \in \mathcal{R}$ irreducible of degree d is at most $N(q, d)$ (This was also proved by Dempwolff (2011))

More isotopisms

More isotopisms

Let $a \in \mathbb{F}_{q^n}^*$ and consider the map $\psi_a \;:\; \mathcal{R} \to \mathcal{R} \;:\; f(t) \mapsto f(at)$

More isotopisms

Let $a \in \mathbb{F}_{q^n}^*$ and consider the map $\psi_a \; : \; \mathcal{R} \to \mathcal{R} \; : \; f(t) \mapsto f(at)$

Lemma

(i) The map ψ_a defines an isomorphism of $\mathcal{R}$.
(ii) If $f \in \mathcal{R}$ is irreducible, then $[\mathbb{S}_f] = [\mathbb{S}_{f^{\psi_a}}]$.
(iii) If $f \in \mathcal{R}$ is irreducible and $mzlm(f) = F(t^n)$, then

$$mzlm(f^{\psi_a}) = \frac{1}{N(a)^d} F(N(a)t^n),$$

where N is the norm from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$.

Bound on the number of isotopism classes of semifields $\mathbb{S}_f$

Define the equiv. relation: $F \sim G \Leftrightarrow \exists \lambda \in \mathbb{F}_q : \; F(X) = G(\lambda X)$.
Put $M(d, q)$:= # equivalence classes of $\sim$ on the set of irreducibles of $\mathbb{F}_q[X]$ of degree d.

Theorem

The number of isotopism classes of semifields $\mathbb{S}_f$ with $f \in \mathcal{R}$ irreducible of degree d is at most $M(q, d)$.

(If q is prime and $(q-1, d) = 1$, $M(q, d) = \frac{N(q,d)}{q-1}$)

Future research

Future research

- Is this bound sharp? Computer data: YES in small cases.

Future research

- Is this bound sharp? Computer data: YES in small cases.
- Can this method be used to count isotopism classes for the generalised cyclic semifields? [JMPT]

Future research

- Is this bound sharp? Computer data: YES in small cases.
- Can this method be used to count isotopism classes for the generalised cyclic semifields? [JMPT]
- Or can this method be generalised in another direction?

Future research

- Is this bound sharp? Computer data: YES in small cases.
- Can this method be used to count isotopism classes for the generalised cyclic semifields? [JMPT]
- Or can this method be generalised in another direction?

Thank you for your attention!