A family of semifields of order 729

Stefano Marcugini

joint work with
J. Bierbrauer, D. Bartoli, G. Faina, F. Pambianco

ACCT 2014

Outline

- Semifields
- A family of semifields in odd characteristic
- The case $q = 3^6$
- The case $q = 3^8$

Semifields

short

remove associativity, commutativity from field axioms

Definition: F is a semifield
or: division algebra, if

- $(F, +)$ commutative group
  $(\longrightarrow$ elementary-abelian, order $q = p^n)$
- $(F, *)$ is a loop (no zero divisors)
- The distributive laws hold
- Unit element (if not: presemifield)
- $0 * y = x * 0 = 0$
- (commutative if $x * y = y * x$)

The start

[Dickson, 1905]

Semifields first arose in the study of algebras resembling fields.

[Veblen and Maclaglan-Wedderburn, 1907]

Use semifields to construct non-desarguesian projective planes.

A geometrical characterization

A non-desarguesian projective plane is a translation plane and also the dual of a translation plane if and only if it can be coordinatized by a proper semifield.

The start

[Dickson, 1905]

Semifields first arose in the study of algebras resembling fields.

[Veblen and Maclaglan-Wedderburn, 1907]

Use semifields to construct non-desarguesian projective planes.

A geometrical characterization

A non-desarguesian projective plane is a translation plane and also the dual of a translation plane if and only if it can be coordinatized by a proper semifield.

A notion of equivalence: isotopy

p prime, $F = \mathbb{F}_{p^r}$.

Definition

Presemifields $(F, *)$ and $(F, \circ)$ are isotopic if
$\beta(x \circ y) = \alpha_1(x) * \alpha_2(y)$ for some $\alpha_1, \alpha_2, \beta \in GL(r, p)$

short

Twist both input variables x, y and the output $x * y$
by linear mappings.

This is the right definition

Two semifields coordinatize isomorphic planes if and only if
they are isotopic. [Albert, 1960]

A notion of equivalence: isotopy

p prime, $F = \mathbb{F}_{p^r}$.

Definition

Presemifields $(F, *)$ and $(F, \circ)$ are isotopic if
$\beta(x \circ y) = \alpha_1(x) * \alpha_2(y)$ for some $\alpha_1, \alpha_2, \beta \in GL(r, p)$

short

Twist both input variables x, y and the output $x * y$
by linear mappings.

This is the right definition

Two semifields coordinatize isomorphic planes if and only if they are isotopic. [Albert, 1960]

The known families of finite commutative semifields in arbitrary odd characteristic

- Finite fields 1893
- Dickson 1906
- Albert 1952
- Zha-Kyureghyan-Wang-Bierbrauer 2009: trans-characteristic construction
- Budaghyan-Helleseth 2008, Zha-Wang 2009
- Pott-Zhou

A family of semifields in odd char [Bierbrauer, preprint]

The parameters

p odd prime, $q = p^m, L = \mathbb{F}_q \subset F = \mathbb{F}_{q^2}$.
Let $\overline{x} = x^q$ and $T : F \longrightarrow L$ the trace.
$0 < s < 2m, \sigma = p^s, l \in L^*$ s. t. $-l \notin (L^*)^{\sigma-1}$.
$C_1, C_2 \in F$ s. t. the polynomial

$$P_{C_1,C_2,s}(X) = C_2 X^{\sigma+1} + \overline{C_1} X^{\sigma} + C_1 X + \overline{C_2} \in F[X]$$

has no root z s. t. $z^{q+1} = 1$.

The presemifield $B(p, m, s, l, C_1, C_2)$ of order p^{2m}

$$x + y := x +_F y$$

$$x * y :=$$

$$(1/2)T((C_1 y^{\sigma} + C_2 \overline{y}^{\sigma})x) + (l/2)T((\overline{C_1} y + C_2 \overline{y})x^{\sigma}) + (xy - \overline{xy})/2$$

A family of semifields in odd char [Bierbrauer, preprint]

The parameters

p odd prime, $q = p^m, L = \mathbb{F}_q \subset F = \mathbb{F}_{q^2}$.
Let $\overline{x} = x^q$ and $T : F \longrightarrow L$ the trace.
$0 < s < 2m, \sigma = p^s, l \in L^*$ s. t. $-l \notin (L^*)^{\sigma-1}$.
$C_1, C_2 \in F$ s. t. the polynomial

$$P_{C_1,C_2,s}(X) = C_2 X^{\sigma+1} + \overline{C_1} X^{\sigma} + C_1 X + \overline{C_2} \in F[X]$$

has no root z s. t. $z^{q+1} = 1$.

The presemifield $B(p, m, s, l, C_1, C_2)$ of order p^{2m}

$$x + y := x +_F y$$

$$x * y :=$$

$$(1/2)T((C_1 y^{\sigma} + C_2 \overline{y}^{\sigma})x) + (l/2)T((\overline{C_1} y + C_2 \overline{y})x^{\sigma}) + (xy - \overline{xy})/2$$

A family of semifields in odd char [Bierbrauer, preprint]

The semifield associated to $B(p, m, s, l, C_1, C_2)$

$$x + y := x +_F y$$
$$x \circ y := \beta\big(\gamma(x) * y\big).$$

where $\beta, \gamma \colon F \to F$ are invertible linear mappings defined by

$$1 * \beta(x) = x \ \text{ and } \ \gamma(x) * 1 = 1 * x.$$

The commutative case

[Budaghyan and Helleseth, 2011]

Constructed two families of commutative semifields

These families are contained in the family $B(p, m, s, l, C_1, C_2)$, in the special cases:

$$\{C_1, C_2\} \subset L \text{ and } C_1 = 0,$$

Open question

Does the family $B(p, m, s, l, C_1, C_2)$ contain commutative examples not isotopic to members of the Budaghyan-Helleseth families?

The commutative case

[Budaghyan and Helleseth, 2011]

Constructed two families of commutative semifields

These families are contained in the family $B(p, m, s, l, C_1, C_2)$, in the special cases:

$$\{C_1, C_2\} \subset L \text{ and } C_1 = 0,$$

Open question

Does the family $B(p, m, s, l, C_1, C_2)$ contain commutative examples not isotopic to members of the Budaghyan-Helleseth families?

The commutative case

[Budaghyan and Helleseth, 2011]

Constructed two families of commutative semifields

These families are contained in the family $B(p, m, s, l, C_1, C_2)$, in the special cases:

$$\{C_1, C_2\} \subset L \text{ and } C_1 = 0,$$

Open question

Does the family $B(p, m, s, l, C_1, C_2)$ contain commutative examples not isotopic to members of the Budaghyan-Helleseth families?

The case $B(3, 3, s, l, C_1, C_2)$

The notation

$q = 3^6 = 729$

L is defined by $\epsilon^3 = \epsilon^2 - 1$

F is defined by $\omega^2 = -1$

$x \in F, \;\; x = a + \omega b, a, b \in L, x = (\underbrace{a}_{Re}, \underbrace{b}_{Im})$

The field multiplication in F is then

$$(a, b)(c, d) = (ac - bd, ad + bc).$$

The case $B(3,3,s,l,C_1,C_2)$, isotopism relations

$B(3,3,s,l,C_1,C_2)$ is isotopic to $B(3,3,3+s,l,C_2,C_1)$ and to $B(3,3,3-s,1/l,C_2,\overline{C_1})$.
This shows that we may assume $s=1$.

$l \in L$ is determined only up to its coset $lL^{*(\sigma-1)}$.
This shows that up to isotopy we may choose $l=1$.

It follows from the theory of projective polynomials that the number of pairs (C_1,C_2) satisfying the polynomial condition equals $27\times 26\times 13\times 21 = 191,646$.

The case $B(3,3,s,l,C_1,C_2)$, isotopism relations

$B(3,3,s,l,C_1,C_2)$ is isotopic to $B(3,3,3+s,l,C_2,C_1)$ and to $B(3,3,3-s,1/l,C_2,\overline{C_1})$.
This shows that we may assume $s=1$.

$l \in L$ is determined only up to its coset $lL^{*(\sigma-1)}$.
This shows that up to isotopy we may choose $l=1$.

It follows from the theory of projective polynomials that the number of pairs (C_1,C_2) satisfying the polynomial condition equals $27 \times 26 \times 13 \times 21 = 191,646$.

The case $B(3, 3, s, l, C_1, C_2)$, isotopism relations

$B(3, 3, s, l, C_1, C_2)$ is isotopic to $B(3, 3, 3 + s, l, C_2, C_1)$ and to $B(3, 3, 3 - s, 1/l, C_2, \overline{C_1})$.
This shows that we may assume $s = 1$.

$l \in L$ is determined only up to its coset $lL^{*(\sigma-1)}$.
This shows that up to isotopy we may choose $l = 1$.

It follows from the theory of projective polynomials that the number of pairs (C_1, C_2) satisfying the polynomial condition equals $27 \times 26 \times 13 \times 21 = 191,646$.

The case $B(3,3,1,1,C_1,C_2)$, isotopism relations

Theorem (scalar isotopy)

The pair (C_1, C_2) can be replaced by $(\lambda C_1, \lambda C_2)$ for $0 \neq \lambda \in L$.

Theorem (Galois isotopy)

Let $C_i = (v_i, h_i)$
The pair (C_1, C_2) can be replaced by $(v_1^3, -h_1^3), (v_2^3, -h_2^3)$.

The case $B(3, 3, 1, 1, C_1, C_2)$, isotopism relations

Theorem (diagonal isotopy)

Let $C_i = (v_i, h_i)$ and work with parameters

$$v_+ = v_1 + v_2, v_- = v_1 - v_2, h_+ = h_1 + h_2, h_- = h_1 - h_2.$$

Then, for arbitrary nonzero $k_1, k_2 \in L$, the following substitutions can be performed without affecting isotopy:

$$v_+ \mapsto k_1^{\sigma+1} v_+, v_- \mapsto k_2^{\sigma+1} v_-,$$

$$h_+ \mapsto k_1^{\sigma} k_2 h_+, h_- \mapsto k_1 k_2^{\sigma} h_-$$

$B(3, 3, 1, 1, C_1, C_2)$ is isotopic to $B(3, 3, 1, 1, C_1', C_2')$, where

$$C_1' = -((k_1^4+k_2^4)v_1+(k_1^4-k_2^4)v_2, (k_1^3 k_2+k_1 k_2^3)h_1+(k_1^3 k_2-k_1 k_2^3)h_2)$$

$$C_2' = -((k_1^4-k_2^4)v_1+(k_1^4+k_2^4)v_2, (k_1^3 k_2-k_1 k_2^3)h_1+(k_1^3 k_2+k_1 k_2^3)h_2)$$

The case $B(3, 3, 1, 1, C_1, C_2)$, isotopism relations

Theorem (1)

$B(3, 3, 1, 1, C_1, C_2)$ is isotopic to $B(3, 3, 1, 1, \alpha^{82} C_1, \alpha^4 C_2)$ for all $0 \neq \alpha \in F$.

$C_1 = 0$

C_2 can be multiplied by an arbitrary fourth power
$\Rightarrow C_2 \in \{1, i, 1+i, 1-i\}$.
existence condition $\Rightarrow C_2 \neq i$.
Galois isotopy $\Rightarrow C_2 = i - 1$ and $C_2 = i + 1$ give isotopic presemifields

$B(3, 3, 1, 1, 0, 1)$ commutative
$B(3, 3, 1, 1, 0, 1 - i)$ non-isotopic to commutative

The case $B(3,3,1,1,C_1,C_2)$, isotopism relations

Theorem (1)

$B(3,3,1,1,C_1,C_2)$ is isotopic to $B(3,3,1,1,\alpha^{82}C_1,\alpha^4 C_2)$ for all $0 \neq \alpha \in F$.

$C_1 = 0$

C_2 can be multiplied by an arbitrary fourth power
$\Rightarrow C_2 \in \{1, i, 1+i, 1-i\}$.
existence condition $\Rightarrow C_2 \neq i$.
Galois isotopy $\Rightarrow C_2 = i-1$ and $C_2 = i+1$ give isotopic presemifields

$B(3,3,1,1,0,1)$ commutative
$B(3,3,1,1,0,1-i)$ non-isotopic to commutative

The case $B(3,3,1,1,C_1,C_2)$, isotopism relations

Theorem (1)

$B(3,3,1,1,C_1,C_2)$ is isotopic to $B(3,3,1,1,\alpha^{82}C_1,\alpha^4 C_2)$ for all $0 \neq \alpha \in F$.

$C_1 = 0$

C_2 can be multiplied by an arbitrary fourth power
$\Rightarrow C_2 \in \{1, i, 1+i, 1-i\}$.
existence condition $\Rightarrow C_2 \neq i$.
Galois isotopy $\Rightarrow C_2 = i-1$ and $C_2 = i+1$ give isotopic presemifields

$B(3,3,1,1,0,1)$ commutative
$B(3,3,1,1,0,1-i)$ non-isotopic to commutative

The case $B(3,3,1,1,C_1,C_2)$, isotopism relations

Theorem (2)

$B(3,3,1,1,C_1,C_2)$ is isotopic to $B(3,3,1,1,\alpha\overline{\alpha}^{\sigma}C_1,\alpha^{\sigma+1}C_2)$ for all $0 \neq \alpha \in F$.

$C_1 \neq 0$,

Theorem (2) $\Rightarrow$ C_1 can be multiplyed by an arbitrary square $\Rightarrow$ $C_1 = 1$ or $1 - i$.
diagonal isotopy $\Rightarrow$ $C_1 = 1$.
Galois isotopy, diagonal isotopy, Theorem (1)
$\Rightarrow$ $B(3,3,1,1,1,C_2)$ come in two isotopy classes.

The case $B(3,3,1,1,C_1,C_2)$, isotopism relations

Theorem (2)

$B(3,3,1,1,C_1,C_2)$ is isotopic to $B(3,3,1,1,\alpha\overline{\alpha}^{\sigma}C_1,\alpha^{\sigma+1}C_2)$ for all $0 \neq \alpha \in F$.

$C_1 \neq 0$,

Theorem (2) $\Rightarrow$ C_1 can be multiplyed by an arbitrary square $\Rightarrow$ $C_1 = 1$ or $1 - i$.
diagonal isotopy $\Rightarrow C_1 = 1$.
Galois isotopy, diagonal isotopy, Theorem (1)
$\Rightarrow B(3,3,1,1,1,C_2)$ come in two isotopy classes.

The case $B(3,3,1,1,C_1,C_2)$, isotopism relations

Theorem

Let $A, B \in F^*$ such that $A\overline{A} \neq B\overline{B}$. Then $B(3,3,1,1,0,C_2)$ is isotopic to $B(3,3,1,1,C_1',C_2')$ where

$$C_1' = C_2AB^3 + \overline{C_2A^3B}, C_2' = C_2A^4 + \overline{C_2B^4}.$$

This Theorem gives isotopies between the two (pre)semifields with $C_1 = 0$ and the two (pre)semifields with $C_1 = 1$

The case $B(3,3,1,1,C_1,C_2)$, isotopism relations

Theorem

Let $A, B \in F^*$ such that $A\overline{A} \neq B\overline{B}$. Then $B(3,3,1,1,0,C_2)$ is isotopic to $B(3,3,1,1,C_1',C_2')$ where

$$C_1' = C_2AB^3 + \overline{C_2A^3B},\; C_2' = C_2A^4 + \overline{C_2B^4}.$$

This Theorem gives isotopies between the two (pre)semifields with $C_1 = 0$ and the two (pre)semifields with $C_1 = 1$

The case $B(3, 3, s, l, C_1, C_2)$

The classification, $q = 3^6$

$B(3, 3, 1, 1, 0, 1)$ commutative

$B(3, 3, 1, 1, 0, 1 - i)$ non isotopic to commutative

The case $B(3, 3, s, l, C_1, C_2)$

The (pre)semifield $B(3, 3, 1, 1, 0, 1)$

Commutative, it belongs to the Budaghyan-Helleseth family.

Its autotopism group has order 1248.

The case $B(3, 3, s, l, C_1, C_2)$

The (pre)semifield $B(3, 3, 1, 1, 0, 1)$

The autotopism group has order at least 1248 :

$$x * y = -T(x\overline{y}^3 + x^3\overline{y}) + \overline{xy} - xy.$$

When will $\alpha_1(x) = Ax, \alpha_2(y) = By$ define an autotopism?

The imaginary part $\Rightarrow AB \in L$, equivalently $B = c\overline{A}$ for $c \in L$.
The real part $\Rightarrow$ the condition $c^3A^4 = cA^4 \in L$.
This shows $c = \pm 1$ and there are 4×26 choices for A.

Together with the field automorphisms (generated by $\alpha_1(x) = x^3, \alpha_2(y) = y^3, \beta(z) = z^{3^5}$) this yields an autotopism group of order $26 \times 4 \times 2 \times 6 = 1248$.

The case $B(3, 3, s, l, C_1, C_2)$

The (pre)semifield $B(3, 3, 1, 1, 0, 1 - i)$

Non isotopic to commutative.

Its autotopism group has order 624.

The case $B(3, 3, s, l, C_1, C_2)$

The two semifields are not isotopic to twisted fields [Albert, 1961]

A generalized twisted field of order 3^6 with left and right nucleus of order 3 is isotopic to a presemifield

$$x * y = xy + lx^{\sigma}y^{\tau}$$

Let $\sigma = 3^s, \tau = 3^t$. The nuclei show that s, t are coprime to 6.
Consider autotopisms of the form

$$\alpha_1(x) = Ax, \alpha_2(y) = By, \beta(z) = z/(AB).$$

$A, B \in F^*$ defines an autotopism if and only if $A^{\sigma-1}B^{\tau-1} = 1$.
We can choose B arbitrarily and have then two choices for A
$\Rightarrow$ the twisted field has at least $2 \times (3^6 - 1) = 1456$ autotopisms and is therefore more symmetric than our semifields.

The case $B(3, 3, s, l, C_1, C_2)$

The two semifields are not isotopic to twisted fields [Albert, 1961]

A generalized twisted field of order 3^6 with left and right nucleus of order 3 is isotopic to a presemifield

$$x * y = xy + lx^{\sigma} y^{\tau}$$

Let $\sigma = 3^s, \tau = 3^t$. The nuclei show that s, t are coprime to 6. Consider autotopisms of the form

$$\alpha_1(x) = Ax, \alpha_2(y) = By, \beta(z) = z/(AB).$$

$A, B \in F^*$ defines an autotopism if and only if $A^{\sigma-1}B^{\tau-1} = 1$. We can choose B arbitrarily and have then two choices for A $\Rightarrow$ the twisted field has at least $2 \times (3^6 - 1) = 1456$ autotopisms and is therefore more symmetric than our semifields.

The case $B(3, 3, s, l, C_1, C_2)$

The two semifields are not isotopic to twisted fields [Albert, 1961]

A generalized twisted field of order 3^6 with left and right nucleus of order 3 is isotopic to a presemifield

$$x * y = xy + lx^\sigma y^\tau$$

Let $\sigma = 3^s, \tau = 3^t$. The nuclei show that s, t are coprime to 6. Consider autotopisms of the form

$$\alpha_1(x) = Ax, \alpha_2(y) = By, \beta(z) = z/(AB).$$

$A, B \in F^*$ defines an autotopism if and only if $A^{\sigma-1}B^{\tau-1} = 1$. We can choose B arbitrarily and have then two choices for A $\Rightarrow$ the twisted field has at least $2 \times (3^6 - 1) = 1456$ autotopisms and is therefore more symmetric than our semifields.

The case $B(3, 4, s, l, C_1, C_2)$

The notation

$q = 3^8 = 6561$

L is defined by $\epsilon^4 = \epsilon + 1$

Let $\mu = \epsilon^5$, *order*$(\mu = 16)$

F is defined by $\omega^2 = \mu$

s=2

It gives isotopes of Dickson semifields.

The case $B(3, 4, s, l, C_1, C_2)$

The notation

$q = 3^8 = 6561$

L is defined by $\epsilon^4 = \epsilon + 1$

Let $\mu = \epsilon^5$, *order*$(\mu = 16)$

F is defined by $\omega^2 = \mu$

s=2

It gives isotopes of Dickson semifields.

The case $B(3, 4, s, l, C_1, C_2)$ $s = 1$

$$l = -\mu$$

The classification, $q = 3^8$

$B(3, 4, 1, -\mu, 0, 1)$ commutative, isotopic to the unique Budaghyan-Helleseth semifield of order 3^8

$B(3, 4, 1, -\mu, 1 + \epsilon/\mu^2, 1 + \epsilon/\mu^2)$ non isotopic to commutative

THANKS FOR THE ATTENTION!