Bivariate semifields

Lukas Kölsch

University of South Florida

(joint work with Faruk Göloğlu)

03/30/2023

Semifields

Definition

A (finite) semifield $\mathbb{S} = (S, +, \circ)$ is a finite set S equipped with two operations $(+, \circ)$ satisfying the following axioms.

(S1) $(S, +)$ is a group.

(S2) For all $x, y, z \in S$,

- $x \circ (y + z) = x \circ y + x \circ z$,
- $(x + y) \circ z = x \circ z + y \circ z$.

(S3) For all $x, y \in S$, $x \circ y = 0$ implies $x = 0$ or $y = 0$.

(S4) There exists $\epsilon \in S$ such that $x \circ \epsilon = x = \epsilon \circ x$.

If (S4) does not hold, we call $\mathbb{S}$ a pre-semifield.

Basic properties

If $\circ$ is associative then $\mathbb{S}$ is a finite field (Wedderburn's Theorem).

Every pre-semifield can easily be turned into a semifield using *Kaplansky's trick*.

The additive group of a semifield $(\mathbb{S}, +, \circ)$ is always an elementary abelian p-group.

We can thus identify the additive group of a semifield $\mathbb{S}$ with the additive group of the finite field $\mathbb{F}_{p^n}$.

Connections

Every semifield can be used to construct translation planes.

There is a 1-to-1 relation between semifields and rank-metric codes with certain optimal parameters.

Even constructions of optimal rank-metric codes with other parameters are often based on semifield constructions.

Definition (Isotopy)

Two semifields $\mathbb{S}_1 = (\mathbb{F}_p^n, +, \circ_1)$ and $\mathbb{S}_2 = (\mathbb{F}_p^n, +, \circ_2)$ are *isotopic* if there exist $\mathbb{F}_p$-linear bijections L, M and N of $\mathbb{F}_{p^n}$ satisfying

$$N(x \circ_1 y) = L(x) \circ_2 M(y).$$

Such a triple $\gamma = (N, L, M)$ is called an *isotopism* between $\mathbb{S}_1$ and $\mathbb{S}_2$.

Definition (Autotopism and the Autotopism group)

The autotopism group $\mathrm{Aut}(\mathbb{S})$ of a pre-semifield $\mathbb{S} = (\mathbb{F}_p^n, +, \circ)$ is defined by

$$\mathrm{Aut}(\mathbb{S}) = \{(N, L, M) \in \mathrm{GL}(\mathbb{F}_{p^n})^3 \colon N(x \circ y) = L(x) \circ M(y)\}.$$

Two semifields are isotopic iff the associated projective planes are isomorphic.

Two examples of semifields

Example (Albert, 1961)

Let $K = \mathbb{F}_{p^n}$, $n > 2$, and define $\circ\colon K \to K$ via

$$x \circ y = xy - ax^q y^r,$$

where $a \notin \mathbb{F}_{p^n}^{q-1} \cdot \mathbb{F}_{p^n}^{r-1}$ and q, r are powers of p. Then $\mathbb{S} = (K, +, \circ)$ is a semifield.

Example (Dickson, 1905, bivariate)

Let $K = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ with p odd and define $\circ\colon K \times K \to K$ via

$$(x, y) \circ (u, v) = (xu + a(yv)^q, xv + yu),$$

where a is a non-square in $\mathbb{F}_{p^m}$ and q is a power of p. Then $\mathbb{S} = (K, +, \circ)$ is a (commutative) semifield.

Two big questions in this talk!

Question

How can we decide if different semifields are isotopic or not? In particular, given a family of semifields, can we decide how big the family is?

Question

Can we determine the autotopism group of a semifield family?

For many of the known semifield families these questions have not been solved!

For Albert semifields, we have the following nice result:

Theorem (Biliotti, Jha, Johnson, 1999)

Let $\mathbb{S}_1, \mathbb{S}_2$ be two isotopic Albert semifields defined over $\mathbb{F}_{p^n}$ via the isotopism $\gamma = (N, L, M) \in \mathrm{GL}(\mathbb{F}_{p^n})^3$. Then $\gamma \in \Gamma L(1, \mathbb{F}_{p^n})^3$. In particular, $\mathrm{Aut}(\mathbb{S}_1) \leq \Gamma L(1, \mathbb{F}_{p^n})^3$.

With this result, everything was reduced from $\mathrm{GL}(\mathbb{F}_{p^n})^3$ to $\Gamma L(1, \mathbb{F}_{p^n})^3$ and the equivalence/autotopism group questions could be solved with relative ease.

The theorem says: All isotopisms and autotopisms are "nice" and structured.

...is it possible to get a similar style result for the *bivariate* semifields (like the Dickson semifields)?

Goal

Find a general way to prove (non)-isotopy and compute autotopism groups for all bivariate semifields.

Idea: Two bivariate semifields defined on $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ *should* be isotopic via an isotopism $\gamma \in \Gamma L(2, \mathbb{F}_{p^m})^3$.
Albert semifields are *univariate* $\implies$ isotopisms/autotopism are in $\Gamma L(1, \mathbb{F}_{p^n})^3$.
Bivariate semifields $\implies$ isotopisms/autotopism are in $\Gamma L(2, \mathbb{F}_{p^m})^3$?

Bivariate constructions

We are interested in special bivariate constructions where $K = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ and

$$(x, y) \circ (u, v) = (f(x, y, u, v), g(x, y, u, v)),$$

and f, g are homogeneous of degree $q + 1$ (resp. $r + 1$) where q, r are powers of p.

Example (Dickson, 1905)

$(x, y) \circ (u, v) = (xu + a(yv)^q, xv + yu)$,

...is isotopic to...

$$(x, y) \circ (u, v) = (xu + ayv, xv^{\overline{q}} + y^{\overline{q}}u)$$

via $y, v \mapsto y^{\overline{q}}, v^{\overline{q}}$ where $\overline{q}$ is defined via $q\overline{q} \equiv 1 \pmod{p^m - 1}$.

It turns out almost all bivariate semifields can be written in this way!

Other examples of bivariate semifields

Example (Taniguchi, 2019)

Let $K = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

$$(x,y)\circ(u,v) = ((x^q u+\alpha x u^q)^{q^2} - a(x^q v - \alpha u^q y)^q - b(y^q v+\alpha y v^q), xv+yu),$$

where $q = p^k$ for some $1 \leq k \leq m-1$, $-\alpha$ is not a $(q-1)$-st power, and the projective polynomial $P_{q,a,b}(x) = x^{q+1} + ax - b$ has no roots in $\mathbb{F}_{p^m}$.

..is isotopic to...

$$(x,y)\circ(u,v) = (x^q u+\alpha^{q^2} x u^q - a(xv^q - \alpha^q u y^q) - b(y^q v+\alpha y v^q), xv^{q^2} + y^{q^2} u).$$

Other examples of bivariate semifields

Example (Knuth, 1965)

Let $K = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

$$(x, y) \circ (u, v) = (xu + ay^{\overline{q}} v^{q^2}, yu + x^{\overline{q}} v + by^{\overline{q}} v^q)$$

where $q = p^k$, $\overline{q} = p^{m-k}$, and $x^{q+1} - bx - a$ has no roots in $\mathbb{F}_{p^m}$.

..is isotopic to...

$$(x, y) \circ (u, v) = (x^{q^2} u + ayv^{q^2}, y^q u + x^q v + byv^q).$$

And many more (Zhou-Pott, Budaghyan-Helleseth, Bierbrauer SF....)!

Why this structure?

We are interested in special bivariate constructions where $K = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ and

$$(x, y) \circ (u, v) = (f(x, y, u, v), g(x, y, u, v)),$$

and f, g are homogeneous of degree $q + 1$ (resp. $r + 1$) where q, r are powers of p.

These semifields have some nice autotopisms! Namely, if $L = M = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ then

$$L(x, y) \circ M(u, v) = (a^{q+1} f(x, y, u, v), a^{r+1} g(x, y, u, v)),$$

so (N, L, M) with $N = \begin{pmatrix} a^{q+1} & 0 \\ 0 & a^{r+1} \end{pmatrix}$ is an autotopism for any $a \in \mathbb{F}_{p^m}^{\times}$.

$\Longrightarrow$ These semifields always have a cyclic subgroup in their autotopism group of order $p^m - 1$.

This is the main property we need!

What can we do with this structure?

1. Systematically search for new semifields that have this structure.

2. Use the nice subgroup in the autotopism group to answer the isotopy/autotopism group questions!

Another new bivariate semifield!

Example (Gölöglu, K., 2022)

Let $K = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, m even and set

$$(x,y)\circ(u,v) = (x^q u + xu^q + b(y^q v + yv^q), x^r v + yu^r + (a/b)(yv^r + y^r v)),$$

where p odd, $q = p^k$ for some $1 \leq k \leq m-1$, $r = p^{k+m/2}$, $b \in \mathbb{F}_{p^m}$ is a non-square, $a \in \mathbb{F}^*_{p^{m/2}}$, $m/\gcd(k,m)$ is odd.

We have two coefficients a, b running over large sets. This seems to indicate that this family might be large!

This family is commutative. Not many commutative semifields of odd order have been found so far!

Use the nice subgroup in the autotopism group to answer the isotopy/autotopism group questions!

Isotopy via the autotopism group

Lemma

Assume $\mathbb{S}_1, \mathbb{S}_2$ *are isotopic (pre-)semifields of order* p^n. *Then* $\mathrm{Aut}(\mathbb{S}_1)$ *and* $\mathrm{Aut}(\mathbb{S}_2)$ *are conjugate in* $\mathrm{GL}(\mathbb{F}_{p^n})^3$.

So if one is able to compute the autotopism group, equivalence is usually quite easy! But - determining the autotopism group is very hard in itself. We have not been able to do that!

There is sometimes a way to use the lemma without knowing the autotopism group - if one can identify a large and nice subgroup first. Recall our bivariate semifields have a cyclic subgroup of order $p^m - 1$ in the autotopism group!

Show that two bivariate semifields $\mathbb{S}_1, \mathbb{S}_2$ are not isotopic - in five simple steps!

- Let $H_1 \leq \mathrm{Aut}(\mathbb{S}_1)$, $H_2 \leq \mathrm{Aut}(\mathbb{S}_2)$ with $|H_1| = |H_2| = p^m - 1$ be the nice cyclic autotopism subgroups.
- Choose a suitable prime p' and Sylow p'-groups $S_1 \leq H_1$, $S_2 \leq H_2$.
- Prove that S_1, S_2 are also Sylow p'-groups of $\mathrm{Aut}(\mathbb{S}_1), \mathrm{Aut}(\mathbb{S}_2)$ (key step!)
- If $\gamma^{-1}\,\mathrm{Aut}(\mathbb{S}_1)\gamma = \mathrm{Aut}(\mathbb{S}_2)$ then $\gamma^{-1}S_1\gamma$ is a Sylow subgroup of $\mathrm{Aut}(\mathbb{S}_2)$. So $\gamma^{-1}S_1\gamma$ and S_2 are conjugate in $\mathrm{Aut}(\mathbb{S}_2)$ (by Sylow's theorem)!
- Determine all $\delta \in \mathrm{GL}(\mathbb{F}_{p^n})^3$ such that $\delta^{-1}S_1\delta = S_2$. If all $\delta \notin \mathrm{Aut}(\mathbb{S}_2)$ then S_1, S_2 are not isotopic.

In some sense, checking $\gamma^{-1}\,\mathrm{Aut}(\mathbb{S}_1)\gamma = \mathrm{Aut}(\mathbb{S}_2)$ is reduced to checking $\delta^{-1}S_1\delta = S_2$.

Last step:

Determine all $\delta \in \mathrm{GL}(\mathbb{F}_{p^n})^3$ such that $\delta^{-1} S_1 \delta = S_2$ and check if $\delta \in \mathrm{Aut}(\mathbb{S}_2)$.

Recall $S_1 \leq H_1$, $S_2 \leq H_2$ and H_1, H_2 consist of mappings (N, L, M) where

$$L = M = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \text{ and } N = \begin{pmatrix} a^{q+1} & 0 \\ 0 & a^{r+1} \end{pmatrix}.$$

Some calculations show that one can reduce everything to the case where q, r for the two semifields coincide, i.e. $S_1 = S_2$.

So: Everything is reduced to finding autotopisms δ that satisfy $\delta^{-1} S_1 \delta = S_1$, i.e. $\delta \in N_{\mathrm{GL}(\mathbb{F}_{p^{2m}})^3}(S_1)$.

A straight-forward calculation shows $N_{\mathrm{GL}(\mathbb{F}_{p^{2m}})^3}(S_1) = \Gamma L(2, \mathbb{F}_{p^m})^3$.

From this procedure we get the following result:

Theorem (Göloğlu, K., 2022)

If two sufficiently nice bivariate semifields defined over $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ are isotopic then there exists an isotopism $\gamma = (N, L, M) \in \Gamma L(2, \mathbb{F}_{p^m})^3$ between them.

This simplifies the isotopy question for all nice bivariate semifields.

However, we could NOT prove that *all* isotopisms are in $\Gamma L(2, \mathbb{F}_{p^m})^3$. In particular, we could not prove $\mathrm{Aut}(\mathbb{S}) \leq \Gamma L(2, \mathbb{F}_{p^m})^3$.

Counting...

For many bivariate semifield families this gives precise counts on the sizes. This leads to

Theorem

The number of non-isotopic (commutative) semifields of size p^n in the Göloglu-K. family is around $p^{n/4}$.

The previous best bound for commutative semifields of odd order was quadratic in n (Zhou-Pott semifields)!

This family is thus by far the biggest one (at least for now).
(Göloğlu, F., Kölsch, L.: An exponential bound on the number of non-isotopic commutative semifields. *Transactions of the American Mathematical Society*, 2022.)

Counting...

The same approach applied to the non-commutative bivariate Taniguchi semifield construction:

Theorem

The number of non-isotopic semifields of size p^n in the Taniguchi family is around $p^{n/2+s}$ where s is the largest divisor of $n/2$ with $2s \neq n/2$.

This improves the lower bound for the number of odd order semifields (previous best was around $p^{n/2}$).

(Göloğlu, F., Kölsch, L.: Counting the number of non-isotopic Taniguchi semifields, 2023+. Preprint on arXiv)

In particular, the number of commutative/non-commutative semifields is now reasonably close..

This approach works well to determine isotopy, but we are not able to get any information on the autotopism groups.

Determining the autotopism group of a semifield is equivalent to computing the collineation group of the associated projective plane.

For the bivariate Knuth semifield planes this is an old open conjecture due to Hughes and Albert:

> Our treatment of the collineation group leaves unanswered a number of possibly interesting questions: (1) Since we only determine a sub-normal series for the group, is the group itself amenable to direct computation? (2) What is the transitive structure of the group, and more particularly, what are the transitive constituents on the line at infinity of the autotopism group $\mathfrak{G}$?

Hughes, D.R., Collineation Groups of Non-Desarguesian Planes II. Some Division Algebras, *American Journal of Mathematics*, 1960.

The bivariate Knuth semifields

Let $K = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

Example (Knuth II.i, 1965)

$(x, y) \circ (u, v) = (x^{q^2}u + ayv^{q^2}, y^q u + x^q v + byv^q)$,
where $q = p^k$ for some $1 \leq k \leq m-1$, and the projective polynomial $P_{q,a,b}(x) = x^{q+1} - bx - a$ has no roots in $\mathbb{F}_{p^m}$.

Example (Knuth II.iv, 1965)

$(x, y) \circ (u, v) = (xu - yv, x^q v + by^q v - y^q u)$,
where $q = p^k$ for some $1 \leq k \leq m-1$ and the projective polynomial $P_{q,a,b}(x) = x^{q+1} - bx - a$ has no roots in $\mathbb{F}_{p^m}$.

(Knuth II.ii, iii exist but are equivalent to Knuth II.iv)

Autotopism groups of the Knuth semifields

How we determined the autotopism group of the Knuth semifields:

Different approaches for the different Knuth semifields.

For Knuth II.iv: A very detailed treatment of projective polynomials $P_{q,a,b}(x) = x^{q+1} - bx - a$ was needed.

Key problem: Knowing the number of roots of P in $\mathbb{F}_{p^m}$, what is the number of roots in $\mathbb{F}_{p^{2m}}$?

Autotopism groups of the Knuth semifields

For Knuth II.i. we used a group theoretic approach:

- Determine $H = \mathrm{Aut}(\mathbb{S}) \cap \Gamma L(2, \mathbb{F}_{p^m})$. We want to show $H = \mathrm{Aut}(\mathbb{S})$.
- Prove that H is self-normalizing in $\mathrm{Aut}(\mathbb{S})$.
- Prove that there is a normal subgroup N such that $g^{-1}Hg \cap H = N$ for all $g \in \mathrm{Aut}(\mathbb{S}) \setminus H$.
- Quotient out N. In the quotient group, if $H \neq \mathrm{Aut}(\mathbb{S})$, then $\mathrm{Aut}(\mathbb{S})$ is a Frobenius group with Frobenius complement H.
- Frobenius complements always have cyclic Sylow subgroups (for odd primes), which is not the case for H.

Theorem (Göloğlu, K., 2023+)

If $\mathbb{S}$ is a bivariate Knuth semifield defined over $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, we have $\mathrm{Aut}(\mathbb{S}) \leq \Gamma L(2, \mathbb{F}_{p^m})^3$.

In all cases, we explicitly compute $\mathrm{Aut}(\mathbb{S})$.

Of course, this yields also again precise counts for the Knuth families.

Theorem (Göloğlu, K., 2023+)

There are around p^m non-isotopic Knuth II.i semifields and around p^d non-isotopic Knuth II.iv semifields of order p^{2m} where d is largest divisor of m but not $m/2$.

A brief summary

The solution to the equivalence problem was very nice and general!

Theorem (Göloğlu, K., 2022)

If two sufficiently nice bivariate semifields defined over $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ are isotopic then there exists an isotopism $\gamma = (N, L, M) \in \Gamma L(2, \mathbb{F}_{p^m})^3$ between them.

Our solution to the autotopism groups heavily uses the structure of the Knuth semifields and cannot be generalized easily.

Question

Is it possible to find a framework that yields a proof that $\mathrm{Aut}(\mathbb{S}) \leq \Gamma L(2, \mathbb{F}_{p^m})^3$ for all (sufficiently nice) bivariate semifields defined over $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$?

A brief summary

We know:

Theorem (Biliotti, Jha, Johnson, 1999)

Let $\mathbb{S}_1, \mathbb{S}_2$ be two isotopic Albert semifields defined over $\mathbb{F}_{p^n}$ with isotopism $\gamma = (N, L, M)$. Then $\gamma \in \Gamma L(1, \mathbb{F}_{p^n})^3$. In particular, $\mathrm{Aut}(\mathbb{S}_1) \leq \Gamma L(1, \mathbb{F}_{p^n})^3$.

Is it possible to prove

Theorem (smart people, near(?) future)

Let $\mathbb{S}_1, \mathbb{S}_2$ be two isotopic nice bivariate semifields defined over $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ with isotopism $\gamma = (N, L, M)$. Then $\gamma \in \Gamma L(2, \mathbb{F}_{p^m})^3$. In particular, $\mathrm{Aut}(\mathbb{S}_1) \leq \Gamma L(2, \mathbb{F}_{p^m})^3$.

This would also show why bivariate semifields are special. They are a natural generalization of the Albert semifields.

What else? Is 2 the highest number?

Bivariate semifields: Use $\mathbb{F}_{p^{2m}} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$....

What else? Is 2 the highest number?

Bivariate semifields: Use $\mathbb{F}_{p^{2m}} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$....

Trivariate semifields?: Use $\mathbb{F}_{p^{3m}} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$....

What else? Is 2 the highest number?

Bivariate semifields: Use $\mathbb{F}_{p^{2m}} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$....

Trivariate semifields?: Use $\mathbb{F}_{p^{3m}} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$....

Multivariate semifields???: Use $\mathbb{F}_{p^{km}} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \times \cdots \times \mathbb{F}_{p^m}$.

What else? Is 2 the highest number?

Bivariate semifields: Use $\mathbb{F}_{p^{2m}} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$....

Trivariate semifields?: Use $\mathbb{F}_{p^{3m}} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$....

Multivariate semifields???: Use $\mathbb{F}_{p^{km}} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \times \cdots \times \mathbb{F}_{p^m}$.

Problem: We knew a lot of examples of bivariate semifields. No examples yet are known for tri-or other multivariate semifields.

What else? Is 2 the highest number?

Bivariate semifields: Use $\mathbb{F}_{p^{2m}} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$....

Trivariate semifields?: Use $\mathbb{F}_{p^{3m}} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$....

Multivariate semifields???: Use $\mathbb{F}_{p^{km}} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \times \cdots \times \mathbb{F}_{p^m}$.

Problem: We knew a lot of examples of bivariate semifields. No examples yet are known for tri-or other multivariate semifields.

(we actually have found some trivariate ones and are working on a paper.)

But: Going from $\Gamma L(1, \mathbb{F}_{p^n})^3$ (Albert) to $\Gamma L(2, \mathbb{F}_{p^m})^3$ (bivariate) was hard and we lost a lot of structure.

Unclear if the approach can be saved.

Future work

Problem (Kantor's conjecture)

Prove that the number of non-isotopic semifields of odd order $N = p^n$ is at least exponential in N.

The best current bound is not linear in N. New general constructions and powerful tools to determine equivalence are needed.

Interestingly, in characteristic 2 a family with exponentially many semifields has been found.

Problem

The autotopism group of any semifield (and thus the collineation group of any semifield plane) is solvable.

We now have more evidence towards this conjecture, but our treatment is too specific.

Thank you for your attention!