Bivariate Semifields and their Isotopies

Lukas Kölsch

University of South Florida

(joint work with Faruk Göloğlu)

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 (pre-)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 (pre-)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.

An example of a semifield

Example (Dickson, 1905)

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 $q = p^k$. Then $\mathbb{S} = (K, +, \circ)$ is a (commutative) semifield.

This is a *bivariate construction*.

There are many bivariate constructions (Zhou-Pott, Budaghyan-Helleseth, Dempwolff, Göloğlu-K.,...).

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 (Göloglu, 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.

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 $a \in \mathbb{F}_{p^m}^{\times}$.

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

Why this structure?

Another reason is: It turns out many of the known bivariate semifields "secretly" have this structure!

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...

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

Why this structure?

Another reason is: It turns out many of the known bivariate semifields semifields "secretly" have this structure!

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, Dickson, Budaghyan-Helleseth, Bierbrauer SF....)!

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 question!

Isotopy of semifields

Question

How can we decide if different semifields are isotopic or not? Can we count the (known) semifields up to isotopy?

Example (Göloglu, 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.

Which choices for q, a, B yield non-isotopic semifields? This is in general a very hard question!

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* $\mathrm{GL}(\mathbb{F}_{p^n})^3$.

Problem: Determining the autotopism group is also very hard!

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 out 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 $H_1 \leq \operatorname{Aut}(\mathbb{S}_1)$, $H_2 \leq \operatorname{Aut}(\mathbb{S}_2)$ 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 $\operatorname{Aut}(\mathbb{S}_1), \operatorname{Aut}(\mathbb{S}_2)$ (key step!)
- If $\gamma^{-1} \operatorname{Aut}(\mathbb{S}_1)\gamma = \operatorname{Aut}(\mathbb{S}_2)$ then $\gamma^{-1} S_1 \gamma$ is a Sylow subgroup of $\operatorname{Aut}(\mathbb{S}_2)$. So $\gamma^{-1} S_1 \gamma$ and S_2 are conjugate in $\operatorname{Aut}(\mathbb{S}_2)$ (by Sylow's theorem)!
- Determine all $\delta \in \operatorname{GL}(\mathbb{F}_{p^n})^3$ such that $\delta^{-1} S_1 \delta = S_2$. If all $\delta \notin \operatorname{Aut}(\mathbb{S}_2)$ then S_1, S_2 are not isotopic.

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

Counting...

We can use this approach to get precise conditions when two bivariate semifields are isotopic or not. This leads to

Theorem

The number of non-isotopic (commutative) semifields of size p^n in the Gölogl u-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).

Counting...

The same appraoch applied to the 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 $p^{n/2}$).

Where to go from here?

Soon: Similar results for the Knuth semifields quadratic over a weak nucleus.

Bonus: Complete determination of the autotopism groups.

Problem (Kantor's conjecture)

Prove that the number of non-isotopic semifields of odd order N is at least superpolynomial in N.

??????? A solution needs a new powerful construction and a way to determine isotopy!

Thank you for your attention!

The talk is based on two papers available on the arXiv:

Göloğlu, F., Kölsch, L.: An exponential bound on the number of non-isotopic commutative semifields. To appear in *Transactions of the American Mathematical Society*. 2022.

Göloğlu, F., Kölsch, L.: Counting the number of non-isotopic Taniguchi semifields.