Counting the number of non-isotopic semifields inside some known semifield families

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 finite field $\mathbb{F}_{p^n}$.

Connections

Every semifield can be used to construct a projective plane.

Commutative semifields in odd characteristic can be used to construct planar/perfect nonlinear functions.

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.

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*.

Other bivariate constructions

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

Let $K = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. Then the following multiplications yield (pre)-semifields:

Example (Taniguchi, 2019)

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

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 $\mathbb{F}_{p^m}$.

Example (Knuth II.i, 1965)

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

where $q = p^k$ for some $1 \leq k \leq m-1$, $q\overline{q} \equiv 1 \pmod{p^m - 1}$, and the projective polynomial $P_{q,a,b}(x) = x^{q+1} + ax - b$ has no roots in $\mathbb{F}_{p^m}$.

Example (Knuth II.iv, 1965)

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

where $q = p^k$ for some $1 \leq k \leq m-1$, $q\overline{q} \equiv 1 \pmod{p^m - 1}$, and the projective polynomial $P_{q,a,b}(x) = x^{q+1} + ax - b$ has no roots in $\mathbb{F}_{p^m}$.

In all those examples, the projective polynomial $P_{q,a,b}(x) = x^{q+1} + ax - b$ is important! We call these semifields *biprojective*.

Equivalences of semifields

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 $\mathbb{S}_2$. If $\mathbb{S}_1 = \mathbb{S}_2$ then γ is called an *autotopism*.

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

Isotopy of semifields is closely related to equivalence of the corresponding planar/perfect nonlinear functions and equivalence of the corresponding rank-metric codes.

Equivalences of functions

Question

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

Example (Taniguchi, 2019)

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

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 $\mathbb{F}_{p^m}$.

Which choices for q, α, a, b yield non-isotopic semifields?

The autotopism group

Definition (Autotopism group)

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

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

Lemma

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

The approach

Problem: Determining the autotopism group is also very hard!

There is often a way to use the lemma without knowing the autotopism group!

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

- Find subgroups $H_1 \leq \mathrm{Aut}(\mathbb{S}_1)$, $H_2 \leq \mathrm{Aut}(\mathbb{S}_2)$ with $|H_1| = |H_2|$.
- Choose a suitable prime r and Sylow r-groups $S_1 \leq H_1$, $S_2 \leq H_2$.
- Prove that S_1, S_2 are also Sylow r-groups of $\mathrm{Aut}(\mathbb{S}_1), \mathrm{Aut}(\mathbb{S}_2)$ (might be hard)
- Show that S_1, S_2 are not conjugate in $\mathrm{GL}(\mathbb{F}_{p^n})^3$.
- Then $\mathrm{Aut}(\mathbb{S}_1)$ and $\mathrm{Aut}(\mathbb{S}_2)$ are also not conjugate in $\mathrm{GL}(\mathbb{F}_{p^n})^3$.

Technique first used to show inequivalence of Boolean functions by Yoshiara (2015), Dempwolff (2016) (power functions).

Generalization to more general classes of Boolean functions and semifields (Göloğlu, K., 2021)

Counting Taniguchi

Theorem (Göloğlu, K., 2022+)

Let $\mathbb{S}_{q,\alpha,a,b}$, $\mathbb{S}_{q,\alpha',a',b'}$ be two Taniguchi semifields of order p^{2m} with $q = p^k$, $k \leq m/2$ and $a, a' \in \{0,1\}$. They are isotopic iff

- *$a = a' = 0$, α/α' is a $(q-1)$-st power and b'^{p^t}/b is a $(q+1)$-st power in $\mathbb{F}_{p^m}^*$.*
- *$a = a' = 1$, $b = b'^{p^t}$ for some $0 \leq t \leq m-1$ and α/α' is a $(q-1)$-st power in $\mathbb{F}_{p^m}^*$.*

The total number of non-isotopic Taniguchi semifields can be precisely determined and is $\approx p^m$.

Counting Knuth semifields...

Similar results are achieved for the Knuth semifields: Let $K = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

Example (Knuth II.i, 1965)

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

where $q = p^k$ for some $1 \leq k \leq m-1$, $q\overline{q} \equiv 1 \pmod{p^m - 1}$, and the projective polynomial $P_{q,a,b}(x) = x^{q+1} + ax - b$ has no roots in $\mathbb{F}_{p^m}$.

Example (Knuth II.iv, 1965)

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

where $q = p^k$ for some $1 \leq k \leq m-1$, $q\overline{q} \equiv 1 \pmod{p^m - 1}$, and the projective polynomial $P_{q,a,b}(x) = x^{q+1} + ax - b$ has no roots in $\mathbb{F}_{p^m}$.

Counting Knuth semifields...

Theorem

There are for a fixed automorphism $q = p^k$ with $\gcd(k, m) = d$ around p^{m-d} non-isotopic Knuth II.i semifields and around p^d non-isotopic Knuth II.iv semifields of order p^{2m}.

These results show that the Taniguchi and the Knuth semifield families are asymptotically around as large as the largest known families of semifields.

Autotopisms

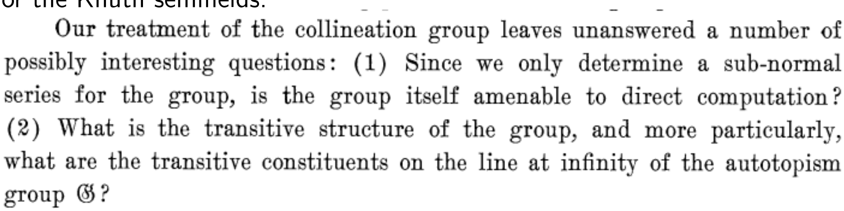
Techniques generalize quite easily to other biprojective semifields (Bierbrauer semifields,. . .).

The main strength of the approach is that it avoids computation of the autotopism group (or something equivalent).

...but the autotopism group is quite interesting in itself! It corresponds to the collineation group of the associated projective plane and the automorphism groups of the associated rank-metric code.

The autotopism group of most semifields is unknown!

For the Knuth semifields:



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 autotopism groups of the Knuth semifields could so far not be determined!

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:

- Find a subgroup H of the autotopism group $\mathrm{Aut}(\mathbb{S})$. 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 $H^g \cap H = N$ 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.

Future work

Problem

Compute the autotopism groups for more semifields.

Problem (Kantor's conjecture)

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

Thank you for your attention!