Semifields, and their relation to cryptography

Lukas Kölsch

University of South Florida

3/2/2023

What is a semifield?

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

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

To define a semifield, it then suffices to specify the "multiplication" $\circ$.

An example of a family of semifields

Example (Twisted fields, 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.

The twisted fields are *commutative* if we choose $q = r$.

Why do we care? - Algebra

Theorem (Wedderburn's theorem)

Every finite domain is a field.

In other words: There is no difference between finite domains, finite division rings, and finite fields.

Semifields are the algebraic structures "closest" to finite fields.

Commutative semifields are especially interesting.

Why do we care? - Algebra

Theorem

There exists (up to isomorphism) exactly one finite field of size p^n *with* p *prime,* $n \geq 1$.

There are more semifields, but they are still *hard to find* (esp. *commutative semifields*)!

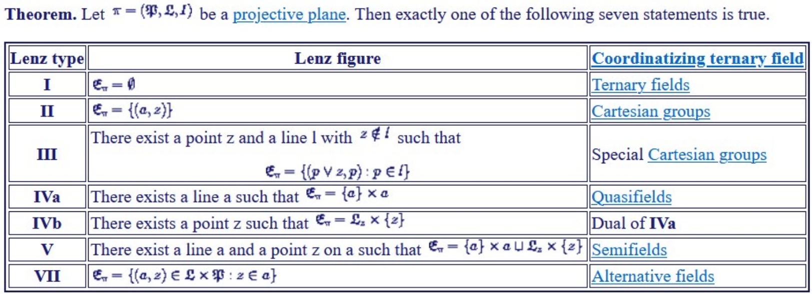
Theorem (Menichetti, 1996)

All semifields of size p^n *with* p, n *prime and* p *large enough are (equivalent to) finite fields or twisted fields.*

Why do we care? - Geometry

Semifields can be used to construct *finite projective planes*.

Projective planes can be divided up into 6 groups based on their symmetries. One of them is derived from semifields.



Theorem. Let $\pi = (\mathfrak{P}, \mathfrak{L}, \mathfrak{I})$ be a projective plane. Then exactly one of the following seven statements is true.

Lenz type	**Lenz figure**	**Coordinatizing ternary field**
I	$\mathfrak{C}_\pi = \emptyset$	Ternary fields
II	$\mathfrak{C}_\pi = \{(a, z)\}$	Cartesian groups
III	There exist a point z and a line l with $z \notin \mathfrak{l}$ such that $\mathfrak{C}_\pi = \{(p \vee z, p) : p \in \mathfrak{l}\}$	Special Cartesian groups
IVa	There exists a line a such that $\mathfrak{C}_\pi = \{a\} \times a$	Quasifields
IVb	There exists a point z such that $\mathfrak{C}_\pi = \mathfrak{L}_z \times \{z\}$	Dual of **IVa**
V	There exist a line a and a point z on a such that $\mathfrak{C}_\pi = \{a\} \times a \sqcup \mathfrak{L}_z \times \{z\}$	Semifields
VII	$\mathfrak{C}_\pi = \{(a, z) \in \mathfrak{L} \times \mathfrak{P} : z \in a\}$	Alternative fields

Constructing semifields ⇔ Constructing projective planes of Lenz type V.

Why do we care? - Coding theory

Semifields can be used to construct *rank-metric codes*.

Definition (Rank-metric code)

Let $M_{n,m}(\mathbb{F}_q)$ the set of $n \times m$-matrices over $\mathbb{F}_q$. A linear *rank-metric code* is a subspace $\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ with minimum distance

$$d = \min_{X,Y \in \mathcal{C}, X \neq Y} \operatorname{rk}(X - Y).$$

The distance used here is the *rank metric*. Main problems:

- Find codes that are "optimal" (achieve maximal $|\mathcal{C}|$ with fixed n, m, d)
- Find for a given $X \in M_{n,m}(\mathbb{F}_q)$ the element in $\mathcal{C}$ closest to X. (decoding problem)

Constructions of rank-metric codes

What is a *good* rank-metric code?

Theorem (Singleton-like bound, Delsarte 1978)

Suppose $\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ *with minimum distance* d. *Then*

$$|\mathcal{C}| \leq q^{n(m-d+1)}.$$

Rank-metric codes satisfying the bound with equality are called maximum rank distance (MRD) code.

There are few constructions of MRD codes and even less have efficient decoding algorithms.

Most constructions of MRD codes are related to *semifields*.

Connecting semifields and MRD codes

We have a simple key connection.

Theorem

Let $\mathbb{S} = (\mathbb{F}_q^n, +, \circ)$ *be a semifield. Then the set of left-multiplications*

$$L_x(y) = x \circ y,\ \mathcal{C} = \{L_x \colon x \in \mathbb{F}_q^n\}$$

defines a linear MRD code with parameters $d = m = n$.

The MRD codes constructed by semifields are *square, full rank* MRD codes.

Note: The distributivity law $x \circ (y + z) = x \circ y + x \circ z$ implies that L_x is a linear mapping.

Connecting semifields and MRD codes

Even more:

Theorem (de la Cruz, Kiermaier, Wassermann, Willems, 2015)

There is a 1-1 correspondence between finite semifields and linear, square full rank MRD codes.

Connecting semifields and MRD codes

Even more:

Theorem (de la Cruz, Kiermaier, Wassermann, Willems, 2015)

There is a 1-1 correspondence between finite semifields and linear, square full rank MRD codes.

And even more: Almost all other known constructions of MRD codes start from a square full rank MRD code - and are thus connected to semifields.

Why do we care? - Code based Cryptography

Rank-metric codes can be used in *code based cryptography*.

Many code-based cryptosystems rely on the hardness of the decoding problem for random codes.

Decoding in the rank-metric is generally considered to be harder than in the classical setting.

Rank-metric code-based cryptography is a new and exciting alternative to classical code-based cryptography.

2 out of 7 second round NIST post-quantum cryptography candidates based on code based cryptography used rank-metric codes.

BUT: Families of good codes like MRD codes need to be constructed.

Objective

Goal

Construct new semifields.

Goal

Give bounds on the total number of semifields.

New semifields give new projective planes and new MRD codes.

Commutative semifields are especially interesting.

Different semifields can be *equivalent*, and we want to construct new examples *up to equivalence*.

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 group)

The autotopism group $\mathrm{Aut}(\mathbb{S})$ of a 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 planes are isomorphic iff the associated rank-metric codes are equivalent.

Bivariate semifields

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

This is a *bivariate construction*.

There are many bivariate constructions!

The known commutative semifields of size p^n, p odd

Until 2022:

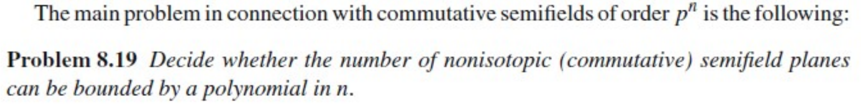
Family	**Count**	Proven in	Bivariate?
The finite field	1	trivial	$\approx$ Yes
Dickson	$\approx n/4$	1905	Yes
Albert's twisted fields	$\approx n/2$	1961	$\approx$ Yes
Ganley	1 ($p = 3$ only)	1981	No
Cohen-Ganley	1 ($p = 3$ only)	1982	No
Coulter-Matthews-Ding-Yuan	2 ($p = 3$ only)	2006	No
Zha-Kyureghyan-Wang	??	2008	No
Budaghyan-Helleseth	$\approx n/2$	2009	Yes
Bierbrauer$_3$	$\approx n/2$	2010	No
Bierbrauer$_4$	$\approx n/2$	2010	No
Zhou-Pott	$\approx n^2$	2013	Yes

The known commutative semifields of size p^n, p odd

Question

How many semifields are there?

Open problem!



The main problem in connection with commutative semifields of order p^n is the following:

Problem 8.19 *Decide whether the number of nonisotopic (commutative) semifield planes can be bounded by a polynomial in n.*

Pott, A.: Almost perfect and planar functions, *Designs, Codes, Cryptography*, 2016.

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.

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

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

where p odd, $q = p^k$, $r = p^{k+m/2}$, $b \in \mathbb{F}_{p^m}$ 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.

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 $p^m - 1$.

Why this structure?

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

Example (Zhou-Pott, 2013)

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

$$(x, y) \circ (u, v) = (x^q u + u^q x + \alpha(y^q v + y v^q)^r, xv + yu)$$

where $q = p^k$, $r = p^l$, $\gcd(k, m)/m$ is odd, and α is a non-square in $\mathbb{F}_{p^m}$.

..is isotopic to...

$$(x, y) \circ (u, v) = (x^q u + u^q x + \alpha(y^q v + y v^q), x^r v + y u^r).$$

And many more (e.g. Dickson, Budaghyan-Helleseth....)!

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?

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, $q = p^k$, $r = p^{k+m/2}$, $a \in \mathbb{F}^*_{p^{m/2}}$, $b \in \mathbb{F}_{p^m}$ is a non-square, $m/\gcd(k, m)$ 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 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 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!

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.

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 $S_1 \leq H_1$, $S_2 \leq H_2$.

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!)

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)!

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 those δ are not isotopisms, then $\mathbb{S}_1$, $\mathbb{S}_2$ are not isotopic.

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

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.*

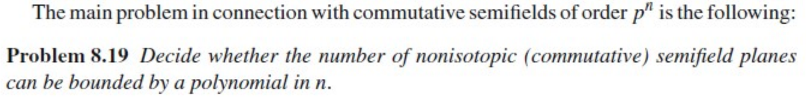
This simplifies the isotopy question for all nice bivariate semifields.

Isotopisms of the form $\gamma = (N, L, M) \in \Gamma L(2, \mathbb{F}_{p^m})^3$ are (comparatively) easy to determine.

The known commutative semifields of size p^n, p odd

Family	**Count**	Proven in	Bivariate?
The finite field	1	trivial	$\approx$ Yes
Dickson	$\approx n/4$	1905	Yes
Albert's twisted Fields	$\approx n/2$	1961	$\approx$ Yes
Ganley	1 ($p = 3$ only)	1981	No
Cohen-Ganley	1 ($p = 3$ only)	1982	No
Coulter-Matthews-Ding-Yuan	2 ($p = 3$ only)	2006	No
Zha-Kyureghyan-Wang	??	2008	No
Budaghyan-Helleseth	$\approx n/2$	2009	Yes
Bierbrauer$_3$	$\approx n/2$	2010	No
Bierbrauer$_4$	$\approx n/2$	2010	No
Zhou-Pott	$\approx n^2$	2013	Yes
Göloğlu-K.	$\approx p^{n/4}$	2022	Yes

The known commutative semifields of size p^n, p odd

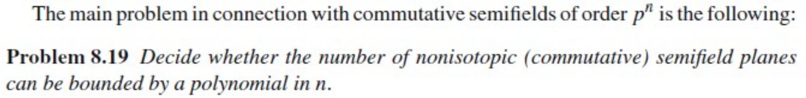


The main problem in connection with commutative semifields of order p^n is the following:

Problem 8.19 *Decide whether the number of nonisotopic (commutative) semifield planes can be bounded by a polynomial in n.*

Pott, A.: Almost perfect and planar functions, *Designs, Codes, Cryptography* (2016)

The known commutative semifields of size p^n, p odd



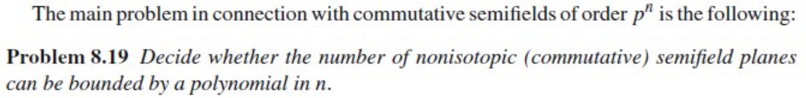
The main problem in connection with commutative semifields of order p^n is the following:

Problem 8.19 *Decide whether the number of nonisotopic (commutative) semifield planes can be bounded by a polynomial in* n.

Pott, A.: Almost perfect and planar functions, *Designs, Codes, Cryptography* (2016)

This problem is now solved!

The known commutative semifields of size p^n, p odd



The main problem in connection with commutative semifields of order p^n is the following:

Problem 8.19 *Decide whether the number of nonisotopic (commutative) semifield planes can be bounded by a polynomial in n.*

Pott, A.: Almost perfect and planar functions, *Designs, Codes, Cryptography* (2016)

This problem is now solved!

This also yields the biggest family of commutative MRD codes and commutative semifield planes!

The known non-commutative semifields of size p^n, p odd

Non-commutative semifields:

- There are more constructions, e.g. via skew-polynomial rings (Petit, 1966), finite geometry (Jha, Johnson, 1990) or secondary constructions based on commutative semifields
- However, counting (up to isotopy) is much more difficult!
- Several families have $\approx p^{n/2}$ non-isotopic elements (Kantor 2003, Lavrauw 2013, Sheekey 2019)

The known non-commutative semifields of size p^n, p odd

Non-commutative semifields:

- There are more constructions, e.g. via skew-polynomial rings (Petit, 1966), finite geometry (Jha, Johnson, 1990) or secondary constructions based on commutative semifields
- However, counting (up to isotopy) is much more difficult!
- Several families have $\approx p^{n/2}$ non-isotopic elements (Kantor 2003, Lavrauw 2013, Sheekey 2019)
- The "square-root barrier" was broken in (Göloğlu, K. , 2023). We presented a family with $\approx p^{2n/3}$ non-isotopic semifields.

Current and future work

Final goal:

Problem (Kantor's conjecture, 2003)

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 $p^{2n/3}$, not even linear in N.

Interestingly, in characteristic 2 a family with exponentially many semifields has been found (Kantor and Williams, 2004).

Current and future work

New constructions:

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

Current and future work

New constructions:

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

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

Current and future work

New constructions:

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 $\mathbb{F}_{p^{km}} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \times \cdots \times \mathbb{F}_{p^m}$.

Current and future work

New constructions:

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 trivariate or other multivariate semifields.

Current and future work

New constructions:

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 trivariate or other multivariate semifields.

Current work: We actually have found some trivariate semifields and are working on a paper.

But: Adapting the group theoretical framework is not as straightforward.

Current and Future work - Coding theory and cryptography

Rank-metric codes from semifields:

- Constructions of MRD codes based on new semifields we found.
- Adapting decoding algorithms of existing MRD codes to new MRD codes.
- Check if cryptosystems using the new codes are resistant to known attacks on rank-metric code based cryptography (e.g. Overbeck's attack).

Shoutouts

Parts of the talk are based on:

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

Göloğlu, F., Kölsch, L.: Counting the number of non-isotopic Taniguchi semifields. To appear in *Designs, Codes, Cryptography*, 2023.

Göloğlu, F., Kölsch, L.: Equivalences of biprojective almost perfect nonlinear functions. To appear in *Journal of Combinatorial Theory, Series A*, 2023.

Kölsch, L., Polujan, A.: Value distributions of perfect nonlinear functions, submitted, 2023.

Thank you for your attention!

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

Göloğlu, F., Kölsch, L.: Counting the number of non-isotopic Taniguchi semifields. To appear in *Designs, Codes, Cryptography*, 2023.

Göloğlu, F., Kölsch, L.: Equivalences of biprojective almost perfect nonlinear functions. To appear in *Journal of Combinatorial Theory, Series A*, 2023.

Kölsch, L., Polujan, A.: Value distributions of perfect nonlinear functions, submitted, 2023.