Semifields and their relations to finite geometry, coding theory, and cryptography

Lukas Kölsch

University of South Florida
Based on joint work with Faruk Göloğlu

03/05/2025 or 03/04/2025
depending on time zone

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 new semifield is *equivalent* to the previous pre-semifield.

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 $(\mathbb{F}_{p^n}, +)$ and just need to define a new multiplication.

Connections

Every semifield $\mathbb{S}$ can be used to construct spreads via the vector spaces

$$V_y = \{(x, x \circ y) \colon x \in \mathbb{S}\} \text{ for } y \in \mathbb{S}$$

and

$$V' = \{(0, y) \colon y \in \mathbb{S}\}.$$

Using the André-Bruck-Bose construction, we get a translation plane from such a *semifield spread*.

In fact, semifield planes are exactly translation planes whose duals are again translation planes.

Explicit construction of affine planes using semifields

Exactly the same construction as the classical construction using a field — substituting field multiplication with *semifield* multiplication.

Affine points: $(a, b) \in \mathbb{S}^2$.

Affine lines: $l_{a,b} = \{(x, a \circ x + b) : x \in \mathbb{S}\}$, $l_c = \{(x, c) : x \in \mathbb{S}\}$

A projective plane can then be constructed by "completing" the affine plane with a line at infinity.

Codes

Classical coding theory is largely concerned with linear codes over a finite field.

Definition (Code)

A linear $[n, k, d]$-code $\mathcal{C} \leq \mathbb{F}_q^n$ is a k-dimensional subspace of $\mathbb{F}_q^n$ such that

$$d = \min_{x,y \in \mathcal{C}, x \neq y} \#\{j \in \{1, \ldots, n\} : x_j \neq y_j\}.$$

The distance used is the *Hamming distance*. Classical problems:

- Find codes that are "optimal" (achieve maximal d with fixed n, k)
- Find for a given point $x \in \mathbb{F}_q^n$ the point in $\mathcal{C}$ closest to x. (decoding problem)

A new approach

We can use *non-classical* coding theory like 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

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

The distance used here is the *rank metric*.

Decoding in the rank metric (seems to be) harder than in the Hamming metric. Possible advantages in cryptosystems!

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.

Connecting semifields and MRD codes

We have a simple key connection.

Theorem

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

$$R_y(x) = x \circ y,\ \mathcal{C} = \{R_y : y \in \mathbb{F}_p^n\}$$

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

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

The MRD codes constructed by semifields are *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.

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: Many known constructions of MRD codes with other arbitrary parameters are related to semifield constructions.

Connections of commutative semifields to difference sets and planar functions

Commutative semifields can be used to construct skew Hadamard difference sets and Paley type partial difference sets (Ding, Yuan, 2006), (Weng, Qiu, Wang, Xiang, 2007).

In particular: Counterexample to the old conjecture that the Paley difference sets are the only examples of skew Hadamard difference sets in abelian groups.

Idea: Replace the set of squares with the set of "semifield squares" $\{x \circ x : x \in \mathbb{S}\}$ for a commutative semifield $\mathbb{S}$.

Commutative semifields also lead to constructions of planar functions that are interesting in symmetric cryptography.

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 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 $\Leftrightarrow$ the associated rank-metric codes are equivalent $\Leftrightarrow$ the associated planes are isomorphic.

Kantor's conjecture

Problem (Kantor's conjecture, 2003)

Prove that the number of non-isotopic semifields of odd order $N = p^n$ is not bounded by a polynomial in N.

The best current bound is $p^{2n/3}$ (Gologlu, K., 2023).

Interestingly, in characteristic 2 a family with exponentially many semifields has been found (Kantor and Williams, 2005).

Equivalently: How many inequivalent square full rank MRD codes are there? How many non-isomorphic semifield planes exist?

Kantor's conjecture

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.

We need:

1. A new, general construction of semifields.
2. A technique to prove non-isotopy between semifields in this family.

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

This is a *bivariate construction*.

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

Biprojective constructions

We are interested in special *biprojective* 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....)!

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, $q = p^k$, $r = p^{k+m/2}$, $B \in \mathbb{F}_{p^m}$ 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 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!

- 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 $\delta^{-1}S_1\delta = S_2$.

From this procedure we get the following result: Two isotopic semifields satisfy $S_1 = S_2$, so the problem is reduced to checking $\delta^{-1} S_1 \delta = S_1$. Recall S_1 is a diagonal matrix with two Singer cycles:

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 symmetric MRD codes!

Applying the same technique to the non-commutative family of Taniguchi semifields yields the best bound for the number of odd characteristic semifields: $\approx p^{2/3n}$ non-isotopic semifields of size p^n (Gologlu, K., 2023)

Bivariate constructions

There are many bivariate semifields, often found using ad hoc constructions based on informed guesses off computer searches.

Question

Is there a way to unify these bivariate constructions?

This might open the door also for generalizations for "multivariate" constructions.

Definition

Let L be a field. An element $T \in \Gamma L(d, L)$ is called irreducible if the only invariant subspaces of T are $\{0\}$ and L^d.

NOTATION: Let $T \in \Gamma L(2, L) \cong \mathrm{GL}(2, L) \rtimes \mathrm{Aut}(L)$ with associated automorphism σ. Then write

$$T = M_T \mathbf{x}^\sigma, \text{ where } M_T \in \mathrm{GL}(2, L).$$

Theorem (Jha, Johnson, 1989)

Let L be a finite field, T be an irreducible element of $\Gamma L(d, L)$. Fix an L-basis of $V = L^d$, say $\{e_0, \ldots, e_{d-1}\}$. Define a multiplication

$$\mathbf{x} \circ \mathbf{y} = \sum_{i=0}^{d-1} y_i T^i(\mathbf{x}),$$

where $\mathbf{y} = \sum_{i=0}^{d-1} y_i e_i$. Then $\mathbb{S}_T = (V, +, \circ)$ is a pre-semifield, called a cyclic semifield.

This construction is equivalent to a construction using skew-polynomial rings.

For $d = 2$ we get bivariate semifields, which are equivalent to the Hughes-Kleinfeld semifields found in 1960.

Is it possible to extend the cyclic semifield construction to cover more known semifields?

Theorem (Sheekey, 2020)

Let $L = \mathbb{F}_{p^n}$ be a field, T be an irreducible element in $\Gamma L(d, \mathbb{F}_{p^n})$ with associated field automorphism σ of order k with fixed field K. Let further ρ be an automorphism of $\mathbb{F}_{p^n}$ with fixed field $K' \leq K$ and $\eta \in L$ chosen such that

$$N_{L:K'}(\eta) N_{K:K'}((-1)^{dk} \det(M_T)) \neq 1$$

Fix an L-basis of $V = L^d$, say $\{e_0, \ldots, e_{d-1}\}$. Define a multiplication

$$\mathbf{x} \circ \mathbf{y} = \sum_{i=0}^{d-1} y_i T^i(\mathbf{x}) + \eta y_0^\rho T^d(\mathbf{x}),$$

where $\mathbf{y} = \sum_{i=0}^{d-1} y_i e_i$. Then $\mathbb{S}_T = (V, +, \circ)$ is a pre-semifield, called a twisted cyclic semifield.

Theorem

Let $L = \mathbb{F}_{p^n}$ be a field, $\mathbf{x}, \mathbf{y} \in L^d$ and T be an irreducible transformation in $\Gamma L(d, \mathbb{F}_{p^n})$ with associated field automorphism σ of order k with fixed field K. Then the mappings $F : L^d \to L^d$ defined by

$$F_{\mathbf{y}}(\mathbf{x}) = \sum_{i=0}^{d-1} y_i T^i(\mathbf{x}) + y_d T^d(\mathbf{x})$$

are non-singular for any $0 \neq \mathbf{y} = (y_1, \ldots, y_{d-1})$ if $y_d = 0$ or

$$N_{L:K}(y_0/y_d) \neq (-1)^{dk} N_{L:K}(\det(M_T)).$$

These are just right-multiplications of the twisted cyclic semifields.

Corollary

Let $L = \mathbb{F}_{p^n}$ be a field, $\mathbf{x} \in L^d$ and T be an irreducible transformation in $\Gamma L(d, \mathbb{F}_{p^n})$ with associated field automorphism σ of order k with fixed field K and inverse $\overline{\sigma}$. Then the mappings $F\colon L^d \to L^d$ defined by

$$F_{y_1,\ldots,y_{d-1}}(\mathbf{x}) = \sum_{i=1}^{d-1} y_i T^{i-1}(\mathbf{x}) + \eta T^{d-1}(\mathbf{x}) + \det(M_T)^{\overline{\sigma}} T^{-1}(\mathbf{x})$$

for any $y_1, \ldots, y_{d-1}$ are non-singular for any $\eta \in L$ with $N_{L:K}(\eta) \neq (-1)^{d(k-1)}$.

Proof.

Compose with T^{-1} and pick coefficients correctly. □

These are A LOT of non-singular mappings! To construct a twisted cyclic semifield, Sheekey fixes a transformation T.

IDEA: We *do not* fix T but change it depending on $y_1, \ldots, y_{d-1}$.

Construction (Construction 1)

Let $L = \mathbb{F}_{p^m}$, $V = L^2$, $\mathbf{x}, \mathbf{y} \in L^2$ with $\mathbf{y} = \binom{y_0}{y_1}$ and σ be a field automorphism of L with fixed field K and $\overline{\sigma}$ its inverse. Further, let $T_a \in \Gamma L(2, L)$, $a \in L^*$ be irreducible transformations satisfying $T_a + T_b = T_{a+b}$ for any $a, b \in L$ where we set $T_0 = T_0^{-1} = 0$. Then

$$\mathbf{x} \circ \mathbf{y} = y_0\mathbf{x} + \eta T_{y_1}(\mathbf{x}) + \det(M_{T_{y_1}})^{\overline{\sigma}} T_{y_1}^{-1}(\mathbf{x})$$

defines a presemifield for any $\eta \in L$ with $N_{L:K}(\eta) \neq 1$.

Proof.

No zero divisors: Assume $\mathbf{x} \circ \mathbf{y} = 0$. If $y_1 = 0$ then $y_0\mathbf{x}$.

If $y_1 \neq 0$, then use Sheekey for $d = 2$. □

A slight variation:

Construction (Construction 2)

Let $V = L^2$, $\mathbf{x}, \mathbf{y} \in V$ with $\mathbf{y} = \binom{y_0}{y_1}$. Let further σ be a field automorphisms of L with fixed field K. Further, let $T_a \in \Gamma L(2, L)$, $a \in L^*$ be irreducible transformations satisfying $T_a + T_b = T_{a+b}$ for any $a, b \in L$, where we set $T_0 = 0$. Then

$$\mathbf{x} \circ \mathbf{y} = y_0\mathbf{x} + T_{y_1}(\mathbf{x})$$

defines a presemifield.

Definition

We call a mapping $\mathcal{T}\colon L \to \Gamma L(2, L) \cup \{0\}$ admissible if

1. $\mathcal{T}(0) = 0$,
2. $\mathcal{T}(a) + \mathcal{T}(b) = \mathcal{T}(a + b)$ for any $a, b \in L$,
3. $\mathcal{T}(a) \in \Gamma L(2, L)$ is irreducible for all $a \in L^*$.

These sets immediately produce semifields via the constructions.

A trivial admissible mapping

Definition

We call a mapping $\mathcal{T}\colon L \to \Gamma L(2, L) \cup \{0\}$ admissible if

1. $\mathcal{T}(0) = 0$,
2. $\mathcal{T}(a) + \mathcal{T}(b) = \mathcal{T}(a + b)$ for any $a, b \in L$,
3. $\mathcal{T}(a) \in \Gamma L(2, L)$ is irreducible for all $a \in L^*$.

Fix irreducible $T \in \Gamma L(2, L)$. Then set $\mathcal{T}(a) = aT$.

This admissible mapping together with the construction just returns Sheekey's twisted cyclic semifields.

2-dimensional irreducible semilinear transformations

We need to find "better", more interesting admissible mappings. To do this, we need to understand irreducible semilinear transformations better.

Proposition

The transformation $T \in \Gamma L(2, L)$ with associated $M_T = \left(\begin{smallmatrix} 0 & \alpha \\ 1 & \beta \end{smallmatrix}\right) \in \mathrm{GL}(2, L)$ and field automorphism σ is irreducible if and only if $X^{\sigma+1} - \beta X - \alpha = 0$ has no solutions in L.

This is a sufficient classification since it is enough to classify up to $\mathrm{GL}(2, L)$-conjugacy (by isotopy).

Proposition (Admissible mapping 1)

Define $\mathcal{T}: L \to \Gamma L(2, L) \cup \{0\}$ *such that* $\mathcal{T}(0) = 0$ *and for* $a \neq 0$ *define* $\mathcal{T}(a) \in \Gamma L(2, L)$ *with associated field automorphism* σ *and associated matrix* $M_a \in \mathrm{GL}(2, L)$ *via*

$$M_a = \begin{pmatrix} 0 & a\alpha \\ a^\tau & 0 \end{pmatrix}$$

for an arbitrary, nontrivial field automorphism τ*. Write* $\sigma: x \mapsto x^{p^k}$*,* $\tau: x \mapsto x^{p^l}$*,* $0 \leq k, l < m$*. Then* $\mathcal{T}$ *is admissible if and only if either*

- α *is a non-square; and* $k = 0$ *or* $\gcd(m, l)/\gcd(m, k, l)$ *is odd; or*
- $k \neq 0$*,* α *is not a* $(p^{\gcd(m,k,l)} + 1)$*-st power and* $\gcd(m, l)/\gcd(m, k, l)$ *is even.*

Proposition (Admissible set 2)

Define $\mathcal{T}: L \to \Gamma L(2, L) \cup \{0\}$ *such that* $\mathcal{T}(0) = 0$ *and for all* $a \neq 0$ *let* $\mathcal{T}(a) \in \Gamma L(2, L)$ *with associated field automorphism* σ *via*

$$M_a = \begin{pmatrix} 0 & a\alpha \\ a^{\sigma^2} & a^{\sigma}\beta \end{pmatrix}.$$

Then $\mathcal{T}$ *is admissible if and only if* $P(X) = X^{\sigma+1} - \beta X - \alpha \in L[X]$ *has no roots in* L.

Recreating known semifields

Family	**Construction**	**Admissible Mapping**	**Notes**
(Generalized) Dickson	Construction 2	Admissible Mapping 1	—
Knuth I	Construction 2	Admissible Mapping 2	—
Knuth II,III,IV, Hughes-Kleinfeld	Construction 2	trivial	—
Bierbrauer, Budaghyan-Helleseth	Construction 1	trivial	Contains comm. SF
Dempwolff	Construction 1	trivial	—
Zhou-Pott	Construction 1	Admissible Mapping 1	—
Taniguchi	Construction 1	Admissible Mapping 2	Largest known construction
(Twisted) cyclic semifields	Constructions 1, 2	trivial	only covers $d = 2$

Table: Known infinite families of semifields of order p^{2m} and how to recreate them

Some new semifields

We also find new semifields using Construction 1, Admissible mapping 1. They are equivalent to a SF on L^2 with multiplication:

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \circ \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_1 y_1^\sigma - \eta x_1^\sigma y_1 + \alpha(x_0 y_0^\sigma - \eta x_0^\sigma y_0) \\ x_0^\tau y_1 + x_1 y_0^\tau \end{pmatrix}.$$

for suitably chosen $\eta, \alpha \in L$, $\sigma, \tau \in \mathrm{Gal}(L)$. For $\eta = -1$ we get the commutative Zhou-Pott semifields.

Recall $\sigma : x \mapsto x^{p^k}$, so these new semifields are *also biprojective*. The previous techniques apply!

Theorem (K., 2025+)

Let $\mathbb{S}_1 = (L^2, +, \circ_1) = \mathbb{S}_{\sigma,\tau,\alpha_1,\eta_1}$ *and* $\mathbb{S}_2 = (L^2, +, \circ_2) = \mathbb{S}_{\sigma_2,\tau_2,\alpha_2,\eta_2}$ *be two semifields defined on* L^2 *with* $\sigma\colon x \mapsto x^{p^k}$, $\tau\colon x \mapsto x^{p^l}$, $k, l < m/2$ *and* $k \neq l$. *Let* K *be the fixed field of* σ. $\mathbb{S}_1$ *and* $\mathbb{S}_2$ *are isotopic if and only if* $\sigma_2 = \sigma$, $\tau_2 = \tau$, *and there exists a field automorphism* ρ *of* L *such that*

- $N_{L:K}(\eta_1)^\rho = N_{L:K}(\eta_2)$, *and*
- $\frac{\alpha_1^\rho}{\alpha_2} \in L^{\sigma+1}L^{\tau-1}$.

In particular, if $N_{L:K}(\eta) \neq N_{L:K}(-1)$ our SF are not isotopic to Zhou-Pott semifields.

One can show that the new family of semifields contains SF not contained in any known family of semifields.

Multivariate semifields

This gives a good explanation of (almost all) bivariate semifields!

Still not enough for Kantor's conjecture...

We cannot just look at degree 2 extensions.

$\Rightarrow$ Search for multivariate Semifields

Multivariate semifields

Let $q = p^m$ and define $F\colon \mathbb{F}_q^3 \to \mathbb{F}_q^3$ via $F(x, y, z) = (f, g, h)$, where $f, g, h\colon \mathbb{F}_q^3 \to \mathbb{F}_q$ are

$$\begin{aligned} f(x, y, z) &= x^{\sigma+1} + ay^\sigma z + bx^\sigma y + cx^\sigma z, \\ g(x, y, z) &= ay^{\sigma+1} + z^\sigma x + bz^\sigma y + cx^\sigma y, \\ h(x, y, z) &= z^{\sigma+1} - x^\sigma y. \end{aligned}$$

Theorem (Gologlu, K., 2025+)

Let $a, b, c \in \mathbb{F}_q$ be such that

$$X^{\sigma^2+\sigma+1} + cX^{\sigma^2+\sigma} + bX^{\sigma^2} + a = 0$$

has no solution $X \in \mathbb{F}_q$. Then $\mathbf{x} \circ \mathbf{y} = F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})$ defines a multiplication of a commutative presemifield.

Let $F\colon \mathbb{F}_q^3 \to \mathbb{F}_q^3$ via $F(x,y,z) = (f,g,h)$, where $f,g,h\colon \mathbb{F}_q^3 \to \mathbb{F}_q$ are

$$\begin{aligned} f(x,y,z) &= x^{\sigma+1} + ay^\sigma z + bx^\sigma y + cx^\sigma z, \\ g(x,y,z) &= ay^{\sigma+1} + z^\sigma x + bz^\sigma y + cx^\sigma y, \\ h(x,y,z) &= z^{\sigma+1} - x^\sigma y. \end{aligned}$$

This was found using educated guesses and a computer search.
Note: f,g,h are homogeneous, so same techniques as earlier can be applied and all isotopisms between semifields in the family are necessarily semilinear over $\mathbb{F}_q$.

We can prove this family contains some previously known family of semifields.

We cannot generalize (yet). Equivalence is (still) hard.

Summary

Problem (Kantor's conjecture, 2003)

Prove that the number of non-isotopic semifields of odd order $N = p^n$ is not bounded by a polynomial in N.

We need:

1. A new, general construction of semifields. We found some, but not enough.
2. A technique to prove non-isotopy between semifields in this family. We found one, but still not enough (?).

What else is to be done.

Rank-metric codes: The twisted cyclic semifields can be embedded into MRD codes with different parameters in a very nice way. Is the same true for our semifields?

What else is to be done.

Rank-metric codes: The twisted cyclic semifields can be embedded into MRD codes with different parameters in a very nice way. Is the same true for our semifields?

In geometry: Semifields define projective planes. Since these semifields are constructed in similar ways; can the planes be treated in a unifying way? Can we find geometric structures (ovals,...).

What else is to be done.

Rank-metric codes: The twisted cyclic semifields can be embedded into MRD codes with different parameters in a very nice way. Is the same true for our semifields?

In geometry: Semifields define projective planes. Since these semifields are constructed in similar ways; can the planes be treated in a unifying way? Can we find geometric structures (ovals,...).
Can we somehow generalize our nice construction to $d > 2$ (i.e. start with semilinear transformations in $\Gamma L(d, L)$ with $d > 2$ —"multivariate constructions").

Thank you for your attention!

The talk is 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. *Designs, Codes, Cryptography*, 2023.

Kölsch, L.: A unifying construction of semifields of order p^{2m}. Preprint, 2024 (on arxiv).

. . . and ongoing projects with Faruk Göloğlu (Charles Univ. Prague).