A unifying construction of semifelds of order p^{2m}

Lukas Kölsch

University of South Florida
Based on joint work with Faruk Göloğlu

01/23/2025

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 $\mathbb{S}$ 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.

Connections

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.

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)

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.

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.

Semifields are spaces of full rank matrices

It is useful to view semifields via their right multiplications $R_y = x \circ y$.
By the semifield properties,

$$\mathcal{S} = \{R_y : y \in \mathbb{S}\},$$

is a subspace of full rank matrices (note $R_{y_1+y_2} = R_{y_1} + R_{y_2}$).
Dually, every subspace of square full rank matrices satisfying the Singleton bound defines a semifield.

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 $T \in \Gamma L(2, L)$ 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 semifield, called a cyclic semifield.

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.

Proof.

We only show that $\mathbb{S}_T$ has no zero divisors.

Define $R_{\mathbf{y}}(\mathbf{x}) = \mathbf{x} \circ \mathbf{y}$. We need to show that $R_{\mathbf{y}}$ has full rank for $\mathbf{y} \neq 0$. □

Proof.

Assume $\mathbf{x} \circ \mathbf{y} = 0$ and $\mathbf{y} \neq 0$. Then there is a $k < d$ such that $y_k \neq 0$ and

$$\sum_{i=0}^{k-1} y_i T^i(\mathbf{x}) = -y_k T^k(\mathbf{x}).$$

So $T^k(\mathbf{x}) \in \langle \mathbf{x}, T(\mathbf{x}), \ldots, T^{k-1}(\mathbf{x}) \rangle$, and $\langle \mathbf{x}, T(\mathbf{x}), \ldots, T^{k-1}(\mathbf{x}) \rangle$ is a T-invariant subspace. □

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

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

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.

This construction covers Albert's semifields as well (for $d = 1$).

Observation: For $d = 2$, this construction covers a bivariate semifield construction of Bierbrauer (2015) - but not other ones.

Theorem (Sheekey, 2020)

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 $F\colon L^d \to L^d$ 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

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

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 $N_{L:K}(\eta) \neq (-1)^{d(k-1)}$.

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.

Assume $\mathbf{x} \circ \mathbf{y} = 0$. If $y_1 = 0$ then $y_0\mathbf{x}$.

If $y_1 \neq 0$, then use Sheekey. □

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 produce semifields via the Construction.

Note: We use subspaces of irreducible transformations in $S \subseteq \Gamma L(2, L)$ of dimension n to construct subspaces of invertible mappings of dimension $2n$.

A trivial admissible mappings

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.

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

What does "recreating semifields" mean?— Isotopy

We can find *equivalent* semifields using our 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 $\mathbb{S}_2$.

What does "recreating semifields" mean? — Knuth orbit

If $(\mathbb{F}_p^n, +, \circ)$ is a semifield, then so is its *dual* $(\mathbb{F}_p^n, +, *)$ where

$$x * y := y \circ x.$$

Moreover, if $\mathbb{S}$ is a semifield, then we can take the dual of its spread. This spread will again define a semifield $\mathbb{S}^t$, called the *transpose* of $\mathbb{S}$.

Taking the dual and taking the transpose induce an S_3-action on the set of semifields, i.e., one semifield will give 6 semifields by taking duals and transposes.

This is called the *Knuth orbit of a semifield.*

Semifields in the same Knuth orbit are in general *not isotopic*.

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.

Theorem

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.

Proof uses some group theoretic ideas developed in previous papers.

Using nuclei arguments, one can show that the new family of semifields contains SF not contained in any known family of semifields.

Summary

Combining the two constructions, together with the two non-trivial admissible mappings, we can generate a ton of semifields.

Summary

Combining the two constructions, together with the two non-trivial admissible mappings, we can generate a ton of semifields.
We cover constructions by: Dickson, Knuth, Bierbrauer, Dempwolff, Budaghyan-Helleseth, Taniguchi, Zhou-Pott, and construct many new examples.

Summary

Combining the two constructions, together with the two non-trivial admissible mappings, we can generate a ton of semifields.
We cover constructions by: Dickson, Knuth, Bierbrauer, Dempwolff, Budaghyan-Helleseth, Taniguchi, Zhou-Pott, and construct many new examples.
In particular: Taniguchi's family is the largest known family of semifields in odd characteristic! So our constructions are *the most powerful constructions* known so far.

Summary

Combining the two constructions, together with the two non-trivial admissible mappings, we can generate a ton of semifields.
We cover constructions by: Dickson, Knuth, Bierbrauer, Dempwolff, Budaghyan-Helleseth, Taniguchi, Zhou-Pott, and construct many new examples.
In particular: Taniguchi's family is the largest known family of semifields in odd characteristic! So our constructions are *the most powerful constructions* known so far.
We also show that there is simple and unifying structure for all these semifields.

What is to be done.

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 is to be done.

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?

Some MRD codes based on (twisted) cyclic semifields have efficient decoding. Now that we understand the structure, can we transfer some of these ideas?

What is to be done.

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?

Some MRD codes based on (twisted) cyclic semifields have efficient decoding. Now that we understand the structure, can we transfer some of these ideas?

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 is to be done.

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?

Some MRD codes based on (twisted) cyclic semifields have efficient decoding. Now that we understand the structure, can we transfer some of these ideas?

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 to $d > 2$ (i.e. start with semilinear transformations in $\Gamma L(d, L)$ with $d > 2$).

What is to be done.

There are bivariate semifields that are not covered by our constructions:

Theorem (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.*

What is different about these semifields? Are more general constructions possible?

Thank you for your attention!