A general and unifying construction for semifields and their related maximum rank distance codes

Lukas Kölsch

University of South Florida

02/26/2024

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 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 (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.

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 right-multiplications

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

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_z is a linear mapping.

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

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 sqaure full rank matrices satisfying the Singleton bound defines a semifield.
Often, MRD codes "contain" semifields (in some cases this is necessary (Sheekey 2019)).

Cyclic semifields

Definition

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

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.

For $d = 2$ we get bivariate semifields, which are equivalent to the Hughes-Kleinfeld semifield 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

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

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 and only 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 (K.,202?)

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 semifield 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. □

Definition

Let L be a finite field. We call a subset $S \subseteq \Gamma L(2, L)$ admissible if

$$S = \{T_a : a \in L^*\} \cup \{\mathbf{0}\}$$

satisfies $T_a + T_b = T_{a+b}$ for any $a, b \in L$ and T_a 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 set

Definition

Let L be a finite field. We call a subset $S \subseteq \Gamma L(2, L)$ admissible if

$$S = \{T_a : a \in L^*\} \cup \{\mathbf{0}\}$$

satisfies $T_a + T_b = T_{a+b}$ for any $a, b \in L$ and T_a is irreducible for all $a \in L^*$.

Let T be irreducible. Then set $T_a = aT$, i.e.

$$S_T = \{aT : a \in L^*\} \cup \{\mathbf{0}\} \subseteq \Gamma L(2, L).$$

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

2-dimensional irreducible semilinear transformations

We need to find "better", more interesting admissible sets. To do this, we need to understand irreducible semilinear transformations better. Let $T \in \Gamma L(2, L)$ with associated automorphism σ. Then write

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

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 set 1)

Let $L = \mathbb{F}_{p^m}$ be a finite field and define $T_a \in \Gamma L(2, L)$ with associated field automorphism σ via

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

for an arbitrary field automorphism τ. Write $\sigma\colon x \mapsto x^{p^k}$, $\tau\colon x \mapsto x^{p^l}$, $0 \leq k, l < m$. Then

$$S_{\alpha,\sigma,\tau} = \{T_a\colon a \in L^*\} \cup \{0\}$$

is admissible if and only if either

- *α is a nonsquare, 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)

Let L be a finite field and define $T_a \in \Gamma L(2, L)$ with associated field automorphism σ via

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

Then

$$S = \{T_a \colon a \in L^*\} \cup \{0\}$$

is admissible if and only if $f = X^{\sigma+1} - \beta X - \alpha \in L[X]$ has no roots in L.

Summary

I found a second construction similar to the one I showed earlier, again based on Sheekey's lemma.

Summary

I found a second construction similar to the one I showed earlier, again based on Sheekey's lemma.

Then combining the two constructions, together with the two non-trivial admissible sets, we can generate a ton of semifields.

Summary

I found a second construction similar to the one I showed earlier, again based on Sheekey's lemma.
Then combining the two constructions, together with the two non-trivial admissible sets, 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

I found a second construction similar to the one I showed earlier, again based on Sheekey's lemma.
Then combining the two constructions, together with the two non-trivial admissible sets, 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

I found a second construction similar to the one I showed earlier, again based on Sheekey's lemma.
Then combining the two constructions, together with the two non-trivial admissible sets, 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.

This is work in progress!

What is to be done.

This is work in progress!

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.

This is work in progress!

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.

This is work in progress!

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.

This is work in progress!

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 is ONE bivariate semifield that is 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 this semifield? Are more general constructions possible?

Thank you for your attention!