Semifields and MRD Codes: Invariants of Interest

John Sheekey

UCD

Irsee, August 2022

Fields and Their Friends

Finite Fields underpin a large portion of Finite Geometry.

Every finite field has prime power order, and there is a unique field (up to isomorphism) of each prime power order.

Some applications of finite fields do not require all the axioms of a field.

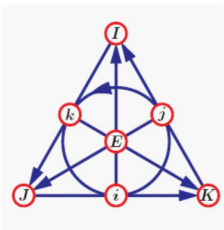
Wedderburn-Dickson Theorem

Every finite associative division algebra is a finite field.

Finite Semifields

A finite semifield $\mathbb{S}$ is a finite division algebra, where multiplication is not assumed to be commutative or associative.

The first constriction of a proper infinite semifield was the octonions by John T. Graves (1843).



×	*i*	*j*	*k*	*E*	*I*	*J*	*K*
i	−1	*k*	−*j*	*I*	−*E*	−*K*	*J*
j	−*k*	−1	*i*	*J*	*K*	−*E*	−*I*
k	*j*	−*i*	−1	*K*	−*J*	*I*	−*E*
E	−*I*	−*J*	−*K*	−1	*i*	*j*	*k*
I	*E*	−*K*	*J*	−*i*	−1	−*k*	*j*
J	*K*	*E*	−*I*	−*j*	*k*	−1	−*i*
K	−*J*	*I*	*E*	−*k*	−*j*	*i*	−1

Dickson (1905) constructed the first examples of proper finite semifields.

Finite Semifields

A finite semifield $\mathbb{S}$ is a finite division algebra, where multiplication is not assumed to be commutative or associative.

Semifields have been studied from a number of different points of view, with a wide variety of motivations.

Each of these settings tells us something different, has its own advantages and disadvantages, provides different techniques, and suggests "natural" sets of problems.

Semifields are related to every part of MATHS.

Finite Semifields

Semifields are related to every part of MATHS.

- M is for Matrices
- A is for Algebra
- T is for Tensors
- H is for Heometry
- S is for Spreads

Finite Semifields

Theorem (Albert/Andre/Maduram/Knuth)

Let $\mathbb{S}_1, \mathbb{S}_2$ be two semifields. The following are equivalent:

- M: The matrix subspaces $C(\mathbb{S}_i)$ are equivalent*;
- A: The algebras $\mathbb{S}_i$ are isotopic;
- T: The tensors $T(\mathbb{S}_1)$ are equivalent*;
- H: The projective planes $\pi(\mathbb{S}_i)$ are isomorphic;
- S: The spreads $\mathcal{S}(\mathbb{S}_i)$ are equivalent.

Although the classification problem is equivalent in each setting, each one suggests different interesting classes of semifields that are worthy of further study!

A is for Algebra

We regard $\mathbb{F}_{q^n}$ as an $\mathbb{F}_q$-vector space of dimension n, and define a new multiplication.

Every $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^n}$ can be represented by a unique linearized polynomial with coefficients in $\mathbb{F}_{q^n}$:

$$f(x) = f_0 x + f_1 x^q + \cdots + f_{n-1} x^{q^{n-1}}$$

For every $\mathbb{F}_q$-bilinear map (multiplication) from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ to $\mathbb{F}_{q^n}$ there exist unique $c_{ij} \in \mathbb{F}_{q^n}$ such that

$$x \circ y = \sum_{i,j=0}^{n-1} c_{ij} x^{q^i} y^{q^j}.$$

A is for Algebra

In general it is very difficult to determine whether or not a multiplication defines a semifield. However in some cases it is straightforward.

Albert's *Generalised Twisted Fields* (1961) use the elements of $\mathbb{F}_{q^n}$, with multiplication defined as

$$x \circ y = xy - cx^{q^i} y^{q^j},$$

with c fixed such that $c^{\frac{q^n-1}{q-1}} \neq 1$.

For suppose $x \circ y = 0$ with $x, y \neq 0$. Then $c = x^{1-q^i} y^{1-q^j}$. Taking the *field norm* of both sides contradicts the condition on c.

A is for Algebra

Equivalence

Two semifields are *isotopic* if there exist invertible additive maps A, B, C such that $(x \star y)^A = x^B \circ y^C$ for all x, y.

- If we do not assume a multiplicative identity, the structure is called a *presemifield*.
- Every presemifields is isotopic to a semifield, via *Kaplansky's trick*.

Question

Can we classify semifields up to isotopy?

A is for Algebra

Classifications

Dickson (1905)

Every semifield two-dimensional over its centre is isotopic to a field

Menichetti (1977)

Every semifield three-dimensional over its centre is isotopic to either a field or generalised twisted field.

Menichetti (1998)

Every semifield of prime dimension over its centre $\mathbb{F}_q$ with q large enough is isotopic to either a field or generalised twisted field.

A is for Algebra

Classifications

Many semifields have been constructed by many authors, such as:

- Dickson
- Hughes-Kleinfeld
- Knuth
- Cohen-Ganley
- Coulter-Matthews
- Jha-Johnson
- Dempwolff
- Kantor
- Budaghyan-Helleseth
- various subsets of [Ebert-Johnson-Marino-Polverino-Trombetti-Lunardon-Lavrauw]
- Zha-Kyureghyan-Wang
- Bierbrauer
- Pott-Zhou
- Bartoli-Bierbrauer-Kyureghyan-Giulietti-Marcugini-Pambianco
- JS
- Gologlu-Kolsch

and many more...

A is for Algebra

Classifications

n	q	#Classes	Reference
4	2	3 (3)	Knuth 1965
4	3	27 (12)	Dempwolff 2008
4	4	(28)	Rua et al 2011
4	5	(42)	Rua et al 2011
4	7	(120)	Rua et al 2012
5	2	6 (3)	Walker 1962
5	3	23 (9)	Rua et al 2011
6	2	332 (80)	Rua et al 2009

x=number of isotopy classes, (x)=number of Knuth orbits

Of the 332 isotopy classes of order 2^6, only 35 were from known constructions.

A is for Algebra

Equivalence

- Constructing semifields is hard...
- Distinguishing semifields from one another is hard...
- Classifying all semifields is hard...

Studying semifieds can be in some sense NP hard...

Studying semifieds can be in some sense NP hard...
they make you want to study a New Problem!

A is for Algebra

Equivalence

Two semifields are *isotopic* if there exist invertible additive maps A, B, C such that $(x \star y)^A = x^B \circ y^C$ for all x, y.

- Determining whether or not two semifields are isotopic is in general very difficult.
- Instead we usually try to come up with some values or properties that are isotopy invariants.
- If two semifields have equal invariants, it does not necessarily imply they are isotopic, but if any of their invariants are different then they are not isotopic.

Isotopy Invariants

Two semifields are *isotopic* if there exist invertible additive maps A, B, C such that $(x \star y)^A = x^B \circ y^C$ for all x, y.

Whenever we define an isotopy invariant we should ask ourselves the following questions:

- Is the invariant easy to calculate?
- How fine or coarse is the invariant?
- What does the invariant tell us about the semifield?
- Can we classify all examples with given invariants?

A is for Algebra

Nuclei and centre

The left, middle and right nucleus are defined as

$$N_l = \{a \in \mathbb{S} \mid (ab)c = a(bc)\ \forall b, c \in \mathbb{S}\}$$
$$N_m = \{b \in \mathbb{S} \mid (ab)c = a(bc)\ \forall a, c \in \mathbb{S}\}$$
$$N_r = \{c \in \mathbb{S} \mid (ab)c = a(bc)\ \forall a, b \in \mathbb{S}\}$$

The centre is the largest field over which $\mathbb{S}$ is a division algebra.

The nuclei are all division rings, and centre is a field. Their sizes are isotopy invariants.

Question

Can we classify semifields with given centre and nuclei?

A is for Algebra

Nuclei and centre

Cardinali-Polverino-Trombetti (2006)

Full classification of semifields four-dimensional over their centre and two-dimensional over a nucleus.

Marino-Polverino-Trombetti (2007) and more

Partial classification of semifields six-dimensional over their centre and two-dimensional over a nucleus.

Blokhuis-Ball-Lavrauw (2003); Lavrauw (2006)

Full classification of commutative semifields two-dimensional over a nucleus for q large enough.

A is for Algebra

Nuclei and centre

- Is the invariant easy to calculate? Yes!
- How fine or coarse is the invariant? Pretty coarse...
- Can we classify all examples with given invariants? Sometimes!

Sometimes calculating the nuclei is sufficient to show that a new construction is not equivalent to an old one; e.g. (Pott-Zhou), (JS).

More often, calculating the nuclei narrows down the list of possible candidates, but further work is required to determine newness.

A is for Algebra

BEL rank

Every semifield multiplication can be written in the form

$$x \circ y = \sum_{k=1}^{r} f_k(x) g_k(y)$$

for some $\mathbb{F}_q$-linear maps f_k, g_k, where r is the rank of the matrix (c_{ij}).

We define the BEL-rank (Lavrauw-JS) of a semifield as the minimum across the isotopy class.

Every generalised twisted field has BEL-rank two, as does every semifields two-dimensional over a nucleus.

The BEL-rank is difficult to calculate, but does give rise to some interesting questions and connections.

A is for Algebra

BEL rank

Question

Can we classify semifields of BEL-rank two?

- Equivalently: disjoint linear sets on a projective line.
- Some computational results give unknown examples of order 2^6.
- Some nonexistence results (JS-Van de Voorde-Voloch, Zini-Zullo).
- Given a semifield of BEL-rank two, we can easily construct another that may or may not be isotopic to it via *switching* (Ball-Ebert-Lavrauw).
- Also related to a construction of planar functions (Pott-Zhou).

A is for Algebra

Commutativity

- Although associativity implies commutativity, the converse is not true.
- Commutative semifields have been extensively studied due to connections with PN functions.
- The function $f(x) = x \circ x$ perfect nonlinear if $\circ$ is commutative and q is odd.
- Semifields of the form $x \circ y = xL(y) + L(x)y$ have been studied (e.g. Kyureghyan-Ozbudak). This corresponds precisely to finding PN functions of the form $xL(x)$.
- Computational classifications for dimension 4 over the centre (Lavrauw-Rodgers, Lavrauw-Sheekey) seem to suggest that a full classification is possible for small dimension, though new ideas are needed.

M is for Matrices

"Multiplication on the left by y" defines a map on $\mathbb{F}_{q^n}$:

$$x \mapsto y \circ x =: L_y(x)$$

Then for $x, z \in \mathbb{F}_{q^n}$, $\lambda \in \mathbb{F}_q$,

$$L_y(x + \lambda z) = L_y(x) + \lambda L_y(z)$$
$$L_{y+\lambda z}(x) = L_y(x) + \lambda L_z(x).$$

- Each L_y is an $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^n}$, and so can be identified with an element of $M_n(\mathbb{F}_q)$.
- The set $C(\mathbb{S}) = \{L_y : y \in \mathbb{F}_{q^n}\}$ is an n-dimensional subspace of $M_n(\mathbb{F}_q)$.
- Each L_y is invertible for $y \neq 0$.

M is for Matrices

The space $C(\mathbb{S})$ is called a (semifield) spread set.

A basis for $C(\mathbb{F}_{2^4})$ over $\mathbb{F}_2$ is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$= \{1, M, M^2, M^3\},$$

where M is the companion matrix of an irreducible polynomial $x^4 + x + 1$ of degree four in $\mathbb{F}_2[x]$.

M is for Matrices

The space $C(\mathbb{S})$ is called a (semifield) spread set.

We can define and study a multivariate polynomial

$$f_{\mathbb{S}}(x_1, \ldots, x_n) = \det\left(\sum_i x_i E_i\right),$$

where $\{E_i\}$ is an $\mathbb{F}_q$-basis for $C(\mathbb{S})$.

The polynomial $f_{\mathbb{S}}$ is homogeneous of degree n in n variables, and has no $\mathbb{F}_q$-rational points.

Menichetti used this approach in his classification results, but not much has been explored in this direction since.

M is for Matrices

Rank Metric Codes

An additively closed subset $\mathcal{C}$ of $M_{m\times n}(\mathbb{F}_q)$ of size q^k such that $\mathrm{rank}(A) \geq d$ for all $0 \neq A \in \mathcal{C}$ and

$$k = \begin{cases} m(n-d+1) & \text{if } m \leq n \\ n(m-d+1) & \text{if } m \geq n \end{cases}$$

is called a *Maximum Rank Distance code*; MRD code for short. We call d the *minimum distance*.

- Studied and constructed by Delsarte (1978) for coding and combinatorial reasons, independently by Gabidulin (1985) for cryptographic reasons.
- The case $d = m = n$ corresponds precisely to semifields.

M is for Matrices

Rank Metric Codes

Some computational results seem to suggest that semifields are more common than MRD codes with $d < n$.

q	n	d	Equiv
2	4	4	3
2	4	3	1
2	5	5	3
2	5	4	2
2	6	6	332
2	6	5	2
3	4	4	27
3	4	3	6

Further results for rectangular matrices (Honold-Kiermaier-Kurz).

M is for Matrices

Constructing Semifields

Let q be a power of an odd prime p, and k a non-square in $\mathbb{F}_{q^m}$.

Then the the finite field $\mathbb{F}_{q^{2m}} \simeq \mathbb{F}_{q^m}[x]/(x^2 - k)$ can be represented as

$$C(\mathbb{F}_{q^{2m}}) = \left\{ \begin{bmatrix} a & kb \\ b & a \end{bmatrix} : a, b \in \mathbb{F}_{q^m} \right\}; \quad \det(L_{a,b}) = a^2 - kb^2$$

Dickson (1906) showed that

$$C(\mathbb{S}) = \left\{ \begin{bmatrix} a & kb^q \\ b & a \end{bmatrix} : a, b \in \mathbb{F}_{q^m} \right\}; \quad \det(L_{a,b}) = a^2 - kb^{p+1}$$

gives a semifield of size q^{2m} with centre $\mathbb{F}_q$, right nucleus $\mathbb{F}_{q^m}$, not equivalent to a field (unless $m = 1$).

M is for Matrices

Nuclei

If $n = sm$ and the right-nucleus of $\mathbb{S}$ has order q^m, then we can assume (up to isotopy) that

$$C(\mathbb{S}) \subset M_s(\mathbb{F}_{q^m}) \subset M_n(\mathbb{F}_q).$$

$C(\mathbb{S})$ is an $\mathbb{F}_q$-subspace of $M_s(\mathbb{F}_{q^m})$

- Via the q-projective system/linear set viewpoint on rank-metric codes, we can thus view a semifield as a rank-metric code in a second way;
- An s^2-dimensional $\mathbb{F}_{q^m}$-linear code in $(\mathbb{F}_{q^m})^{ms}$.
- More generally an $\mathbb{F}_q$-linear rank-metric code in $M_{s\times t}(\mathbb{F}_{q^m})$ of dimension k defines an st-dimensional $\mathbb{F}_{q^m}$-linear rank-metric code in $(\mathbb{F}_{q^m})^k$.

M is for Matrices

Nuclei

$C(\mathbb{S})$ is an $\mathbb{F}_q$-subspace of $M_s(\mathbb{F}_{q^m})$

- Isotopic semifields define equivalent codes in this setting, but non-isotopic semifields can define equivalent codes; thus this alternative viewpoint can act as a useful isotopy invariant.
- Though they didn't use this language, this is the approach used by Cardinali, Polverino. Trombetti, Marino, Johnson, Ebert, Lavrauw in classifications of semifields two-dimensional over a nucleus and four/six-dimensional over the centre.

M is for Matrices

Equivalence

$C(\mathbb{S})$ is an $\mathbb{F}_q$-subspace of $M_s(\mathbb{F}_{q^m})$

Two $\mathbb{F}_q$-subspaces C_1, C_2 of $M_s(\mathbb{F}_{q^m})$ are *equivalent* if there exist $A, B \in \mathrm{GL}(s, q^m)$, $\rho \in \mathrm{Aut}(\mathbb{F}_{q^m})$ such that $C_2 = AC_1^{\rho}B$.

We have the action of a group

$$\mathrm{GL}(s, q^m) \times \mathrm{GL}(s, q^m) \times \mathrm{Aut}(\mathbb{F}_{q^m}) \leq \Gamma\mathrm{L}(s^2, q^m),$$

the stabiliser of a Segre variety. Thus subgroup preserves rank; the isometries in the rank-metric.

M is for Matrices

and H is for Geometry

Given $C(\mathbb{S})$ an $\mathbb{F}_q$-subspace of $M_s(\mathbb{F}_{q^m})$, we can consider geometric properties that are invariant under isotopy.

In particular, how does $C(\mathbb{S})$ intersect the $\mathbb{F}_{q^m}$-subspaces of $M_s(\mathbb{F}_{q^m})$?

Effectively, we check whether $C(\mathbb{S})$ are equivalent under the action of $\Gamma\mathrm{L}(s^2, q^m)$, rather than the subgroup of rank-preserving maps.

M is for Matrices

and H is for Geometry

For example the Dickson semifields:

$$C(\mathbb{S}) = \left\{ \begin{bmatrix} a & kb^p \\ b & a \end{bmatrix} : a, b \in \mathbb{F}_q \right\}$$

Then

$$\alpha \begin{bmatrix} a & kb^p \\ b & a \end{bmatrix} \in C(\mathbb{S}) \Leftrightarrow b(\alpha^q - \alpha) = 0.$$

Hence $C(\mathbb{S})$ contains one 1-dimensional $\mathbb{F}_{q^m}$-subspace, and meets every other 1-dimensional $\mathbb{F}_{q^m}$-subspace either trivially or in a 1-dimensional $\mathbb{F}_q$-subspace.

M is for Matrices

and H is for Geometry

Suppose $s = 2$ and $m = 3$.

(0) L is a union of either q^2+q+1 or q^2+1 lines of a pencil in Σ.
(1) L is a union of q^2+q+1 lines in a plane not belonging to a pencil.
(2) L is a union of q^2+q+1 lines through a point, not all lines in the same plane.
(3) L contains a unique point of weight 2, does not contain any line and is not contained in a plane.
(4) L contains exactly one line and such a line contains $q+1$ points of weight 2.
(5) Any point of L has weight 1 (that is, L is a scattered $\mathbb{F}_q$-linear set).

The corresponding classes of semifields are labeled $\mathcal{F}_i$, for $i = 0, 1, \ldots, 5$. Moreover, in [10] the class $\mathcal{F}_4$ is further partitioned into three subclasses. Namely, if r is the unique line contained in the linear set $L = L(S)$ of type (4), then one of the following situations must occur:

(a) $r^\perp \cap L = \emptyset$,
(b) $|r^\perp \cap L| = 1$,
(c) $|r^\perp \cap L| = q+1$,

where $\perp$ is the polarity of Σ induced by the hyperbolic quadric $\mathcal{Q} \cong \mathrm{Q}^+(3, q^3)$. The corresponding subclasses of semifields are denoted $\mathcal{F}_4^{(a)}$, $\mathcal{F}_4^{(b)}$, and $\mathcal{F}_4^{(c)}$, respectively. We now determine the general form for multiplication in each of these subclasses.

(Ebert-Marino-Polverino-Trombetti)

M is for Matrices

and H is for Geometry

Suppose $s = 2$ and $m = 3$.

Semifields of order q^6 with $|\mathbb{N}_l| = q^3$ and $|\mathbb{K}| = q$

Family	$\lvert\mathbb{N}_m\rvert$	$\lvert\mathbb{N}_r\rvert$	Existence results
$\mathcal{F}_0$	q	q	**Generalized Dickson semifields, q odd**
$\mathcal{F}_1$	q	q	**Semifields from Payne–Thas ovoid of $Q(4,3^3)$**
$\mathcal{F}_2$	q	q	**Semifields from Ganley flock of $PG(3,3^3)$**
$\mathcal{F}_3$	q	q	HJ semifields [9] of type II, III, IV, V for $q = 2$ Dempwolff
$\mathcal{F}_4^{(a)}$	q^2	q	$\exists$! **semifield for q odd,** $\nexists$ **semifields for q even**
	q	q^2	$\exists$! **semifield for q odd,** $\nexists$ **semifields for q even**
	q	q	?
$\mathcal{F}_4^{(b)}$	q	q	There exist semifields for $q = 3$ [7]
$\mathcal{F}_4^{(c)}$	q	q	There exist semifields for any q [6]
	q^2	q^2	**Cyclic semifields for any q**
$\mathcal{F}_5$	q^3	q^3	**Hughes Kleinfeld semifields**
	q^3	q	**Knuth semifields of type (17) for any q**
	q	q^3	**Knuth semifields of type (19) for any q**
	q^2	q	$\exists$ for any $q \neq 2$ (e.g. Generalized Twisted Fields)
	q	q^2	$\exists$ for any $q \neq 2$ (e.g. Generalized Twisted Fields)
	q	q	$\exists$ for any $q \neq 2$ (e.g. Generalized Twisted Fields)

(Ebert-Marino-Polverino-Trombetti)

M is for Matrices

and H is for Geometry

- For example, if $C(\mathbb{S})$ meets every 1-dimensional $\mathbb{F}_{q^m}$-subspace in an $\mathbb{F}_q$-subspace of dimension at most 1, the semifield is said to be scattered.
- We furthermore have a duality operation; the translation dual, a special case of the more general Delsarte dual operation on MRD codes (Lunardon, JS-Van de Voorde).

Question

What can we say for $s > 2$? Or for MRD codes? Can we construct or classify semifields/MRD codes with extremal intersection properties?

T is for Tensors

By choosing an $\mathbb{F}_q$-basis $\{e_i\}$ for a semifield with centre containing $\mathbb{F}_q$, we can represent the multiplication in a semifield by a 3-dimensional array $T(\mathbb{S})$:

$$e_i \circ e_j = \sum_k T_{ijk} e_k.$$

The cube of elements from $\mathbb{F}_q$ can be obtained by stacking the elements of a basis of $C(\mathbb{S})$.

Knuth(1965)

Permuting the subscripts preserves the property of being a (pre)semifield.

Thus from one semifield we obtain a set of (up to) six isotopy classes, known as the Knuth Orbit.

T is for Tensors

Tensor Rank

Let $V^{\otimes 3} = V \otimes V \otimes V$, where V is an n-dimensional F-vector space.

Every tensor $T \in V^{\otimes 3}$ can be written as a sum of *pure* (or *fundamental*) tensors. We refer to an expression

$$T = \sum_{j=1}^{R} v_{j1} \otimes v_{j2} \otimes v_{j3}$$

as a *decomposition* of T into the sum of R pure tensors.

The *tensor rank* of T is the minimum nonnegative integer R such that there exists a decomposition of T into R pure tensors. It is denoted by $\mathrm{trk}(T)$.

T is for Tensors

Tensor Rank

Liebler (1981) and Lavrauw (Irsee, 2011) proposed studying the tensor representation of semifields, in particular the tensor rank.

The tensor rank of an algebra is an isotopy (and Knuth orbit) invariant.

The tensor rank measures the multiplicative complexity of an algebra.

Question

Do there exist semifields with different tensor rank to the field of the same order?

T is for Tensors

Tensor Rank

Lavrauw-Pavan-Zanella (2013) showed that the fields and twisted fields of dimension 3 over their centre have the same tensor rank.

	$q = 2$		$q = 3$	
n	LB	UB	LB	UB
2	3	3	3	3
3	6	6	6	6
4	9	9	8	9
5	13	13	10	12
6	15	15	12	15
7	18	22	17	19
8	20	24	19	21
9	26	30	21	26
10	28	33	24/25	27

Lower bounds taken from Grassl (codetables.de), Upper bounds taken from Cenk-Ozbudak (2010).

T is for Tensors

Tensor Rank

Theorem (Lavrauw-JS)

The tensor rank of both $\mathbb{F}_{3^4}$ and GTF_{3^4} over $\mathbb{F}_3$ is nine.

The tensor rank of all other semifields of order 3^4 over $\mathbb{F}_3$ is eight.

- The tensor rank is very difficult to calculate.
- We don't know yet how broad the range of ranks may be.
- However, the possible practical applications of a semifield with low multiplicative complexity make this an intriguing direction for semifields.

T is for Tensors

Tensor Rank

- Similar ideas have been explored for rank-metric codes (Byrne-Neri-Ravagnani-JS), where low tensor rank has benefits for efficient storage.
- New calculations of the tensor rank of MRD codes have been performed (Byrne-Cotardo), (Bartoli-Zini-Zullo).
- Further invariants arising from tensors have been defined and explored (Byrne-Cotardo).

S is for Spreads

Given a semifield with multiplication $\circ$, we can define certain n-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}^2$, which we can identify with $\mathbb{F}_q^{2n}$:

$$S_y := \{(x, y \circ x) : x \in \mathbb{F}_{q^n}\}; \quad S_\infty := \{(0, x) : x \in \mathbb{F}_{q^n}\}$$

The set

$$\mathcal{D}(\mathbb{S}) = \{S_y : y \in \mathbb{F}_{q^n} \cup \{\infty\}\}$$

forms a spread of $\mathbb{F}_q^{2n}$; every nonzero vector is contained in precisely one element of $\mathcal{D}(\mathbb{S})$.

S is for Spreads

- Spreads arising from semifields are called semifield spreads.
- They are characterised by the following property: the subgroup of $\mathrm{GL}(2n, q)$ fixing the spread setwise, and fixing one element of the spread elementwise, acts transitively on the rest of the spread.
- This special element S_∞ is called the shears element.

S is for Spreads

- If every element of $\mathcal{D}(\mathbb{S})$ is totally isotropic with respect to a nonsingular symplectic form, the spread is called symplectic.
- This corresponds (indirectly!) to the algebraic notion of commutativity.
- Kantor used the spread approach to construct a large class of commutative semifields, showing that the number of equivalence classes is exponential for q even.

S is for Spreads

Let $\mathcal{D}$ be any collection of subspaces of a vector space.

A subspace U is $(\mathcal{D}, h)$-scattered if $\dim(U \cap S) \leq h$ for all $h \in \mathcal{D}$.

- First studied by Blokhuis-Lavrauw in the case $h = 1$.
- Closely related to evasive subspaces.

(Bartoli-Csajbok-Marino-Trombetti) (Gruica-Ravagnani-JS-Zullo)

If $\mathcal{D}$ is any spread of n-dimensional spaces in $V(mn, q)$, then $\dim(U) \leq n(m-1) + h - 1$.

If $\mathcal{D}$ is a Desarguesian spread, then $\dim(U) \leq \frac{hmn}{h+1}$.

S is for Spreads

And M is for Matrices

Let $\mathcal{D}$ be any collection of subspaces of a vector space.

A subspace U is $(\mathcal{D}, h)$-scattered if $\dim(U \cap S) \leq h$ for all $h \in \mathcal{D}$.

The following are equivalent:

- There exists a $(\mathcal{D}(\mathbb{S}), h)$-scattered subspace of dimension n meeting S_∞ trivially.
- The covering radius of $\mathcal{C}(\mathbb{S})$ is at least $n - h$.

The following are equivalent:

- There exists a $(\mathcal{D}(\mathbb{S}), h)$-scattered subspace of dimension n meeting S_∞ non-trivially.
- The covering radius of $\mathcal{C}(\mathbb{S})^{-1}$ is at least $n - h$.

S is for Spreads

Thus we have two new isotopy invariants for semifields arising from the spread representation; the smallest h for which there exists a $(\mathcal{D}, h)$-scattered subspace (meeting S_∞ trivially or not).

Gruica-Ravagnani-JS-Zullo

For any spread $\mathcal{D}$ there exists a $(\mathcal{D}, \lfloor\sqrt{n+1}\rfloor)$-scattered subspace.

Thus the minimum such h could in theory range between 1 and $\lfloor\sqrt{n+1}\rfloor$.

Question

What range of values actually occur? Can we construct or classify extremal cases?

S is for Spreads

When $q = 2$, we further have that a $(\mathcal{D}(\mathbb{S}), 1)$-scattered subspace of dimension n exists if and only if the projective plane $\pi(\mathbb{S})$ possesses a translation hyperoval.

These have been shown to exist only in a small number of cases; e.g. Knuth's binary semifields (Durante-Trombetti-Zhou). Cherowitzo conjectured that they exist for all spreads.

Allen-JS (in preparation)

The spread of $V(12, 2)$ defined by the generalised twisted field of order 2^6 with nucleus of order 2^2 does not possess any $(\mathcal{D}, 1)$-scattered subspaces of dimension 6.

This disproves Cherowitzo's conjecture, and shows that this invariant is non-trivial.

MATHS is for Semifields

Theorem (Albert/Andre/Maduram/Knuth)

Let $\mathbb{S}_1, \mathbb{S}_2$ be two semifields. The following are equivalent:

- M: The matrix subspaces $C(\mathbb{S}_i)$ are equivalent*;
- A: The algebras $\mathbb{S}_i$ are isotopic;
- T: The tensors $T(\mathbb{S}_1)$ are equivalent*;
- H: The projective planes $\pi(\mathbb{S}_i)$ are isomorphic;
- S: The spreads $\mathcal{S}(\mathbb{S}_i)$ are equivalent.

Although the classification problem is equivalent in each setting, each one suggests different interesting classes of semifields that are worthy of further study!