Commutative Semifields

Morgan Rodgers
(Joint work with Michel Lavrauw)

California State University, Fresno

11 September, 2017

Origin

- Finite semifields are related to many important geometric and combinatorial constructs.
- Commutative semifields are of particular interest, as historically there have been few known examples.
- The problem is approached using the connection between commutative semifields and certain types of linear sets.
- We detail computational results towards classifying examples with rank 2 and 3 over the left nucleus (R2CS and R3CS).

Origin

- Finite semifields are related to many important geometric and combinatorial constructs.
- Commutative semifields are of particular interest, as historically there have been few known examples.
- The problem is approached using the connection between commutative semifields and certain types of linear sets.
- We detail computational results towards classifying examples with rank 2 and 3 over the left nucleus (R2CS and R3CS).

Origin

- Finite semifields are related to many important geometric and combinatorial constructs.
- Commutative semifields are of particular interest, as historically there have been few known examples.
- The problem is approached using the connection between commutative semifields and certain types of linear sets.
- We detail computational results towards classifying examples with rank 2 and 3 over the left nucleus (R2CS and R3CS).

Origin

- Finite semifields are related to many important geometric and combinatorial constructs.
- Commutative semifields are of particular interest, as historically there have been few known examples.
- The problem is approached using the connection between commutative semifields and certain types of linear sets.
- We detail computational results towards classifying examples with rank 2 and 3 over the left nucleus (R2CS and R3CS).

Finite semifields

A **semifield** $\mathbb{S}$ is a possibly non-associative algebra with an identity and no zero divisors.

The **left nucleus** $\mathbb{N}_\ell(\mathbb{S})$ (right, middle) is the set of elements $x \in \mathbb{S}$ such that, for all $y, z \in \mathbb{S}$, $x \circ (y \circ z) = (x \circ y) \circ z$.

The intersection of the left, right, and middle nuclei is called simply the **nucleus**. The intersection of the nucleus with the commutative center is called the **center** $\mathbb{Z}(\mathbb{S})$.

The **dimension** of a semifield is the (vector space) dimension over its center; the **rank** of a semifield is its dimension the left nucleus.

Finite semifields

A **semifield** $\mathbb{S}$ is a possibly non-associative algebra with an identity and no zero divisors.

The **left nucleus** $\mathbb{N}_\ell(\mathbb{S})$ (right, middle) is the set of elements $x \in \mathbb{S}$ such that, for all $y, z \in \mathbb{S}$, $x \circ (y \circ z) = (x \circ y) \circ z$.

The intersection of the left, right, and middle nuclei is called simply the **nucleus**. The intersection of the nucleus with the commutative center is called the **center** $\mathbb{Z}(\mathbb{S})$.

The **dimension** of a semifield is the (vector space) dimension over its center; the **rank** of a semifield is its dimension the left nucleus.

Finite semifields

A **semifield** $\mathbb{S}$ is a possibly non-associative algebra with an identity and no zero divisors.

The **left nucleus** $\mathbb{N}_\ell(\mathbb{S})$ (right, middle) is the set of elements $x \in \mathbb{S}$ such that, for all $y, z \in \mathbb{S}$, $x \circ (y \circ z) = (x \circ y) \circ z$.

The intersection of the left, right, and middle nuclei is called simply the **nucleus**. The intersection of the nucleus with the commutative center is called the **center** $\mathbb{Z}(\mathbb{S})$.

The **dimension** of a semifield is the (vector space) dimension over its center; the **rank** of a semifield is its dimension the left nucleus.

Finite semifields

A **semifield** $\mathbb{S}$ is a possibly non-associative algebra with an identity and no zero divisors.

The **left nucleus** $\mathbb{N}_\ell(\mathbb{S})$ (right, middle) is the set of elements $x \in \mathbb{S}$ such that, for all $y, z \in \mathbb{S}$, $x \circ (y \circ z) = (x \circ y) \circ z$.

The intersection of the left, right, and middle nuclei is called simply the **nucleus**. The intersection of the nucleus with the commutative center is called the **center** $\mathbb{Z}(\mathbb{S})$.

The **dimension** of a semifield is the (vector space) dimension over its center; the **rank** of a semifield is its dimension the left nucleus.

Semifield spreads

Semifields can be described in terms of **spread sets** of q^k $k \times k$ matrices over $\mathbb{F}_q$ with nonsingular pairwise differences.

A spread set over $\mathbb{F}_q$ determines a spread $\mathcal{S}$ of $\mathrm{PG}(2k-1, q)$, giving a translation plane $A(\mathcal{S})$ of order q^k.

A spread $\mathcal{S}$ is a **semifield spread** if the spread set is an additive subgroup of $\mathcal{M}_k(q)$, in which case $A(\mathcal{S})$ can be coordinatized by a semifield of order q^k whose left nucleus contains $\mathbb{F}_q$.

A semifield $\mathbb{S}$ is classified according to its isotopism class $[\mathbb{S}]$, isotopic semifields coordinatise isomorphic translation planes.

Semifield spreads

Semifields can be described in terms of **spread sets** of q^k $k \times k$ matrices over $\mathbb{F}_q$ with nonsingular pairwise differences.

A spread set over $\mathbb{F}_q$ determines a spread $\mathcal{S}$ of $\mathrm{PG}(2k-1, q)$, giving a translation plane $A(\mathcal{S})$ of order q^k.

A spread $\mathcal{S}$ is a **semifield spread** if the spread set is an additive subgroup of $\mathcal{M}_k(q)$, in which case $A(\mathcal{S})$ can be coordinatized by a semifield of order q^k whose left nucleus contains $\mathbb{F}_q$.

A semifield $\mathbb{S}$ is classified according to its isotopism class $[\mathbb{S}]$, isotopic semifields coordinatise isomorphic translation planes.

Semifield spreads

Semifields can be described in terms of **spread sets** of q^k $k \times k$ matrices over $\mathbb{F}_q$ with nonsingular pairwise differences.

A spread set over $\mathbb{F}_q$ determines a spread $\mathcal{S}$ of $\mathrm{PG}(2k-1, q)$, giving a translation plane $A(\mathcal{S})$ of order q^k.

A spread $\mathcal{S}$ is a **semifield spread** if the spread set is an additive subgroup of $\mathcal{M}_k(q)$, in which case $A(\mathcal{S})$ can be coordinatized by a semifield of order q^k whose left nucleus contains $\mathbb{F}_q$.

A semifield $\mathbb{S}$ is classified according to its isotopism class $[\mathbb{S}]$, isotopic semifields coordinatise isomorphic translation planes.

Semifield spreads

Semifields can be described in terms of **spread sets** of q^k $k \times k$ matrices over $\mathbb{F}_q$ with nonsingular pairwise differences.

A spread set over $\mathbb{F}_q$ determines a spread $\mathcal{S}$ of $\mathrm{PG}(2k-1, q)$, giving a translation plane $A(\mathcal{S})$ of order q^k.

A spread $\mathcal{S}$ is a **semifield spread** if the spread set is an additive subgroup of $\mathcal{M}_k(q)$, in which case $A(\mathcal{S})$ can be coordinatized by a semifield of order q^k whose left nucleus contains $\mathbb{F}_q$.

A semifield $\mathbb{S}$ is classified according to its isotopism class $[\mathbb{S}]$, isotopic semifields coordinatise isomorphic translation planes.

Knuth orbit and commutativity

The **Knuth orbit** of $\mathbb{S}$ is a collection of at most six isotopism classes $\{[\mathbb{S}], [\mathbb{S}^t], [\mathbb{S}^d], [\mathbb{S}^{td}], [\mathbb{S}^{dt}], [\mathbb{S}^{tdt}]\}$, t and d denote *transpose* and *dual* operations.

Commutativity of a semifield is **not** invariant under isotopism, a semifield $\mathbb{S}$ can be considered "**commutative**" if it is isotopic to a commutative semifield, i.e. if $[\mathbb{S}^d] = [\mathbb{S}]$.

Then the subspaces of the spread associated with $\mathbb{S}^{td}$ are totally isotropic with respect to a symplectic polarity of $\mathrm{PG}(2k-1, q)$, i.e. $\mathbb{S}^{td}$ is a **symplectic** semifield.

Knuth orbit and commutativity

The **Knuth orbit** of $\mathbb{S}$ is a collection of at most six isotopism classes $\{[\mathbb{S}], [\mathbb{S}^t], [\mathbb{S}^d], [\mathbb{S}^{td}], [\mathbb{S}^{dt}], [\mathbb{S}^{tdt}]\}$, t and d denote *transpose* and *dual* operations.

Commutativity of a semifield is **not** invariant under isotopism, a semifield $\mathbb{S}$ can be considered "**commutative**" if it is isotopic to a commutative semifield, i.e. if $[\mathbb{S}^d] = [\mathbb{S}]$.

Then the subspaces of the spread associated with $\mathbb{S}^{td}$ are totally isotropic with respect to a symplectic polarity of $\mathrm{PG}(2k-1, q)$, i.e. $\mathbb{S}^{td}$ is a **symplectic** semifield.

Knuth orbit and commutativity

The **Knuth orbit** of $\mathbb{S}$ is a collection of at most six isotopism classes $\{[\mathbb{S}], [\mathbb{S}^t], [\mathbb{S}^d], [\mathbb{S}^{td}], [\mathbb{S}^{dt}], [\mathbb{S}^{tdt}]\}$, t and d denote *transpose* and *dual* operations.

Commutativity of a semifield is **not** invariant under isotopism, a semifield $\mathbb{S}$ can be considered "**commutative**" if it is isotopic to a commutative semifield, i.e. if $[\mathbb{S}^d] = [\mathbb{S}]$.

Then the subspaces of the spread associated with $\mathbb{S}^{td}$ are totally isotropic with respect to a symplectic polarity of $\mathrm{PG}(2k-1, q)$, i.e. $\mathbb{S}^{td}$ is a **symplectic** semifield.

Linear sets

Under the field reduction map,
points of $\mathrm{PG}(t-1,q^n) \to$ Desarguesian spread of $\mathrm{PG}(tn-1,q)$.

An $\mathbb{F}_q$-**linear set** $\mathcal{L}$ of $\mathrm{PG}(t-1,q^n)$ corresponds to the spread elements intersecting some subspace U of $\mathrm{PG}(tn-1,q)$. The **rank** of $\mathcal{L}$ is $\dim(U)$.

$$\begin{array}{ccc} \text{Semifield } \mathbb{S},\ |\mathbb{S}| = q^{kn} & \longleftrightarrow & \text{Spread set } \mathcal{S} \subseteq \mathrm{PG}(k^2-1,q^n) \\ \mathbb{F}_{q^k} \subseteq \mathbb{N}_\ell(\mathbb{S}),\ \mathbb{F}_q \subseteq \mathbb{Z}(\mathbb{S}) & & \mathbb{F}_q\text{-linear, disjoint from } \mathcal{S}_{k,k}(q^n) \end{array}$$

If $\mathbb{S}$ is symplectic, (WLOG) the matrices of $\mathcal{S}$ are symmetric, contained in a $\left(\frac{k(k+1)}{2}-1\right)$-dimensional subspace intersecting $\mathcal{S}_{k,k}(q^n)$ in a quadratic Veronesean $\mathcal{V}_k$.

Linear sets

Under the field reduction map,
points of $\mathrm{PG}(t-1, q^n) \to$ Desarguesian spread of $\mathrm{PG}(tn-1, q)$.

An $\mathbb{F}_q$-**linear set** $\mathcal{L}$ of $\mathrm{PG}(t-1, q^n)$ corresponds to the spread elements intersecting some subspace U of $\mathrm{PG}(tn-1, q)$. The **rank** of $\mathcal{L}$ is $\dim(U)$.

Semifield $\mathbb{S}$, $\lvert\mathbb{S}\rvert = q^{kn}$	$\longleftrightarrow$	Spread set $\mathcal{S} \subseteq \mathrm{PG}(k^2-1, q^n)$
$\mathbb{F}_{q^k} \subseteq \mathbb{N}_\ell(\mathbb{S})$, $\mathbb{F}_q \subseteq \mathbb{Z}(\mathbb{S})$		$\mathbb{F}_q$-linear, disjoint from $\mathcal{S}_{k,k}(q^n)$

If $\mathbb{S}$ is symplectic, (WLOG) the matrices of $\mathcal{S}$ are symmetric, contained in a $\left(\frac{k(k+1)}{2} - 1\right)$-dimensional subspace intersecting $\mathcal{S}_{k,k}(q^n)$ in a quadratic Veronesean $\mathcal{V}_k$.

Linear sets

Under the field reduction map,
points of $\mathrm{PG}(t-1, q^n) \rightarrow$ Desarguesian spread of $\mathrm{PG}(tn-1, q)$.

An $\mathbb{F}_q$-**linear set** $\mathcal{L}$ of $\mathrm{PG}(t-1, q^n)$ corresponds to the spread elements intersecting some subspace U of $\mathrm{PG}(tn-1, q)$. The **rank** of $\mathcal{L}$ is $\dim(U)$.

$$\begin{array}{ccc} \text{Semifield } \mathbb{S},\ |\mathbb{S}| = q^{kn} & \longleftrightarrow & \text{Spread set } \mathcal{S} \subseteq \mathrm{PG}(k^2-1, q^n) \\ \mathbb{F}_{q^k} \subseteq \mathbb{N}_\ell(\mathbb{S}),\ \mathbb{F}_q \subseteq \mathbb{Z}(\mathbb{S}) & & \mathbb{F}_q\text{-linear, disjoint from } \mathcal{S}_{k,k}(q^n) \end{array}$$

If $\mathbb{S}$ is symplectic, (WLOG) the matrices of $\mathcal{S}$ are symmetric, contained in a $\left(\frac{k(k+1)}{2} - 1\right)$-dimensional subspace intersecting $\mathcal{S}_{k,k}(q^n)$ in a quadratic Veronesean $\mathcal{V}_k$.

Linear sets

Under the field reduction map,
points of $\mathrm{PG}(t-1, q^n) \rightarrow$ Desarguesian spread of $\mathrm{PG}(tn-1, q)$.

An $\mathbb{F}_q$-**linear set** $\mathcal{L}$ of $\mathrm{PG}(t-1, q^n)$ corresponds to the spread elements intersecting some subspace U of $\mathrm{PG}(tn-1, q)$. The **rank** of $\mathcal{L}$ is $\dim(U)$.

$$\begin{array}{ccc} \text{Semifield } \mathbb{S},\ |\mathbb{S}| = q^{kn} & \longleftrightarrow & \text{Spread set } \mathcal{S} \subseteq \mathrm{PG}(k^2-1, q^n) \\ \mathbb{F}_{q^k} \subseteq \mathbb{N}_\ell(\mathbb{S}),\ \mathbb{F}_q \subseteq \mathbb{Z}(\mathbb{S}) & & \mathbb{F}_q\text{-linear, disjoint from } \mathcal{S}_{k,k}(q^n) \end{array}$$

If $\mathbb{S}$ is symplectic, (WLOG) the matrices of $\mathcal{S}$ are symmetric, contained in a $\left(\frac{k(k+1)}{2} - 1\right)$-dimensional subspace intersecting $\mathcal{S}_{k,k}(q^n)$ in a quadratic Veronesean $\mathcal{V}_k$.

Rank 2 commutative semifields

Easiest place to start is with commutative semifields having rank 2 over their left nucleus (R2CS).

Cohen and Ganley showed that any R2CS of order q^{2n} with center $\mathbb{F}_q$, q odd, arises from a pair (f, g) of $\mathbb{F}_q$-linear functions such that $g^2(t) - 4tf(t)$ is a nonsquare for all $t \in \mathbb{F}_{q^n}^*$.

This is equivalent to the existence of a rank n $\mathbb{F}_q$-linear set

$$\mathcal{W} = \{(t, f(t), g(t)) : t \in \mathbb{F}_{q^n}^*\}$$

contained in the set of interior points $\mathcal{I}(\mathcal{C})$ of the conic $\mathcal{C}$ with equation $X_2^2 - 4X_0X_1 = 0$ in $\mathrm{PG}(2, q^n)$.

Rank 2 commutative semifields

Easiest place to start is with commutative semifields having rank 2 over their left nucleus (R2CS).

Cohen and Ganley showed that any R2CS of order q^{2n} with center $\mathbb{F}_q$, q odd, arises from a pair (f, g) of $\mathbb{F}_q$-linear functions such that $g^2(t) - 4tf(t)$ is a nonsquare for all $t \in \mathbb{F}_{q^n}^*$.

This is equivalent to the existence of a rank n $\mathbb{F}_q$-linear set

$$\mathcal{W} = \{(t, f(t), g(t)) : t \in \mathbb{F}_{q^n}^*\}$$

contained in the set of interior points $\mathcal{I}(\mathcal{C})$ of the conic $\mathcal{C}$ with equation $X_2^2 - 4X_0X_1 = 0$ in $\mathrm{PG}(2, q^n)$.

Rank 2 commutative semifields

Easiest place to start is with commutative semifields having rank 2 over their left nucleus (R2CS).

Cohen and Ganley showed that any R2CS of order q^{2n} with center $\mathbb{F}_q$, q odd, arises from a pair (f, g) of $\mathbb{F}_q$-linear functions such that $g^2(t) - 4tf(t)$ is a nonsquare for all $t \in \mathbb{F}_{q^n}^*$.

This is equivalent to the existence of a rank n $\mathbb{F}_q$-linear set

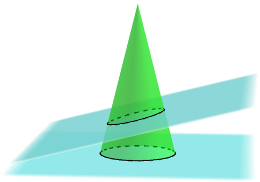
$$\mathcal{W} = \{(t, f(t), g(t)) : t \in \mathbb{F}_{q^n}^*\}$$

contained in the set of interior points $\mathcal{I}(\mathcal{C})$ of the conic $\mathcal{C}$ with equation $X_2^2 - 4X_0X_1 = 0$ in $\mathrm{PG}(2, q^n)$.

Semifield flocks and translation ovoids

These functions f and g give connections to many other important geometric objects. For example

- The functions f and g defining a R2CS determine planes
$$\{\pi_t : tX_0 + f(t)X_1 + g(t)X_2 + X_3 = 0 \mid t \in \mathbb{F}_{q^n}\}$$
in $\mathrm{PG}(3, q^n)$ forming a **semifield flock of a quadratic cone**.

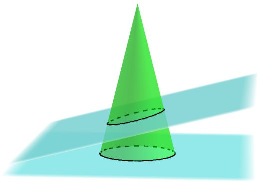


- A semifield flock of a quadratic cone in $\mathrm{PG}(3, q^n)$ is equivalent to a **translation ovoid** of the GQ $\mathcal{Q}(4, q^n)$.

Semifield flocks and translation ovoids

These functions f and g give connections to many other important geometric objects. For example

- The functions f and g defining a R2CS determine planes
$$\{\pi_t : tX_0 + f(t)X_1 + g(t)X_2 + X_3 = 0 \mid t \in \mathbb{F}_{q^n}\}$$
in $\mathrm{PG}(3, q^n)$ forming a **semifield flock of a quadratic cone**.

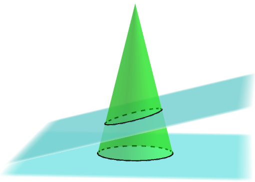


- A semifield flock of a quadratic cone in $\mathrm{PG}(3, q^n)$ is equivalent to a **translation ovoid** of the GQ $\mathcal{Q}(4, q^n)$.

Semifield flocks and translation ovoids

These functions f and g give connections to many other important geometric objects. For example

- The functions f and g defining a R2CS determine planes
$$\{\pi_t : tX_0 + f(t)X_1 + g(t)X_2 + X_3 = 0 \mid t \in \mathbb{F}_{q^n}\}$$
in $\mathrm{PG}(3, q^n)$ forming a **semifield flock of a quadratic cone**.



- A semifield flock of a quadratic cone in $\mathrm{PG}(3, q^n)$ is equivalent to a **translation ovoid** of the GQ $\mathcal{Q}(4, q^n)$.

Known R2CS examples and bounds

There are no R2CS with q even. For q odd, there are very few known examples.

- The Dickson semifields (1906).
- The Cohen-Ganley semifields (1982), which have order 3^{2n} for $n \geq 2$ and center $\mathbb{F}_3$.
- The example found by Penttila and Williams (2000), having order 3^{10} and center $\mathbb{F}_3$.

Known R2CS examples and bounds

There are no R2CS with q even. For q odd, there are very few known examples.

- The Dickson semifields (1906).
- The Cohen-Ganley semifields (1982), which have order 3^{2n} for $n \geq 2$ and center $\mathbb{F}_3$.
- The example found by Penttila and Williams (2000), having order 3^{10} and center $\mathbb{F}_3$.

Known R2CS examples and bounds

There are no R2CS with q even. For q odd, there are very few known examples.

- The Dickson semifields (1906).
- The Cohen-Ganley semifields (1982), which have order 3^{2n} for $n \geq 2$ and center $\mathbb{F}_3$.
- The example found by Penttila and Williams (2000), having order 3^{10} and center $\mathbb{F}_3$.

Known R2CS examples and bounds

There are no R2CS with q even. For q odd, there are very few known examples.

- The Dickson semifields (1906).
- The Cohen-Ganley semifields (1982), which have order 3^{2n} for $n \geq 2$ and center $\mathbb{F}_3$.
- The example found by Penttila and Williams (2000), having order 3^{10} and center $\mathbb{F}_3$.

Structure of linear sets

If the linear set $\mathcal{W}$ associated with an R2CS is contained in a line, then it must be a Dickson semifield; to find new semifields we need linear sets that contain an $\mathbb{F}_q$-subplane.

Theorem (Ball, Blokhuis, Lavrauw 2003; Lavrauw, 2006)

If there exists an $\mathbb{F}_q$-subplane in $\mathrm{PG}(2, q^n)$ contained in $\mathcal{I}(\mathcal{C})$ then there exists an $\mathbb{F}_q$-subline contained in $\ell \cap \mathcal{I}(\mathcal{C})$ with ℓ external to $\mathcal{C}$; such a subline does not exist for

$$q \geq 4n^2 - 8n + 2,$$

or for

$$q > 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$$

when q is prime.

Structure of linear sets

If the linear set $\mathcal{W}$ associated with an R2CS is contained in a line, then it must be a Dickson semifield; to find new semifields we need linear sets that contain an $\mathbb{F}_q$-subplane.

Theorem (Ball, Blokhuis, Lavrauw 2003; Lavrauw, 2006)

If there exists an $\mathbb{F}_q$-subplane in $\mathrm{PG}(2, q^n)$ contained in $\mathcal{I}(\mathcal{C})$ then there exists an $\mathbb{F}_q$-subline contained in $\ell \cap \mathcal{I}(\mathcal{C})$ with ℓ external to $\mathcal{C}$; such a subline does not exist for

$$q \geq 4n^2 - 8n + 2,$$

or for

$$q > 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$$

when q is prime.

Structure of linear sets

If the linear set $\mathcal{W}$ associated with an R2CS is contained in a line, then it must be a Dickson semifield; to find new semifields we need linear sets that contain an $\mathbb{F}_q$-subplane.

Theorem (Ball, Blokhuis, Lavrauw 2003; Lavrauw, 2006)

If there exists an $\mathbb{F}_q$-subplane in $\mathrm{PG}(2, q^n)$ contained in $\mathcal{I}(\mathcal{C})$ then there exists an $\mathbb{F}_q$-subline contained in $\ell \cap \mathcal{I}(\mathcal{C})$ with ℓ external to $\mathcal{C}$; such a subline does not exist for

$$q \geq 4n^2 - 8n + 2,$$

or for

$$q > 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$$

when q is prime.

Outline of the algorithm

This leads us to the following strategy for searching for $2k$-dimensional R2CS:

- Determine values of q for which there actually exists an $\mathbb{F}_q$-subline contained in $\mathcal{I}(\mathcal{C})$ spanning an external line to $\mathcal{C}$ (for some fixed conic $\mathcal{C}$).
- For these values, find all $\mathbb{F}_q$-sublines contained in $\mathcal{I}(\mathcal{C})$ and determine whether there are two which generate a suitable $\mathbb{F}_q$-subplane.
- Use a clique-finding algorithm to determine if subplanes can be combined to give a rank k $\mathbb{F}_q$-linear set contained in $\mathcal{I}(\mathcal{C})$.

Outline of the algorithm

This leads us to the following strategy for searching for $2k$-dimensional R2CS:

- Determine values of q for which there actually exists an $\mathbb{F}_q$-subline contained in $\mathcal{I}(\mathcal{C})$ spanning an external line to $\mathcal{C}$ (for some fixed conic $\mathcal{C}$).
- For these values, find all $\mathbb{F}_q$-sublines contained in $\mathcal{I}(\mathcal{C})$ and determine whether there are two which generate a suitable $\mathbb{F}_q$-subplane.
- Use a clique-finding algorithm to determine if subplanes can be combined to give a rank k $\mathbb{F}_q$-linear set contained in $\mathcal{I}(\mathcal{C})$.

Outline of the algorithm

This leads us to the following strategy for searching for $2k$-dimensional R2CS:

- Determine values of q for which there actually exists an $\mathbb{F}_q$-subline contained in $\mathcal{I}(\mathcal{C})$ spanning an external line to $\mathcal{C}$ (for some fixed conic $\mathcal{C}$).
- For these values, find all $\mathbb{F}_q$-sublines contained in $\mathcal{I}(\mathcal{C})$ and determine whether there are two which generate a suitable $\mathbb{F}_q$-subplane.
- Use a clique-finding algorithm to determine if subplanes can be combined to give a rank k $\mathbb{F}_q$-linear set contained in $\mathcal{I}(\mathcal{C})$.

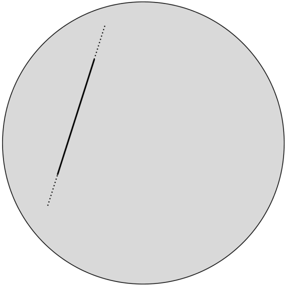
Outline of the algorithm

This leads us to the following strategy for searching for $2k$-dimensional R2CS:

- Determine values of q for which there actually exists an $\mathbb{F}_q$-subline contained in $\mathcal{I}(\mathcal{C})$ spanning an external line to $\mathcal{C}$ (for some fixed conic $\mathcal{C}$).
- For these values, find all $\mathbb{F}_q$-sublines contained in $\mathcal{I}(\mathcal{C})$ and determine whether there are two which generate a suitable $\mathbb{F}_q$-subplane.
- Use a clique-finding algorithm to determine if subplanes can be combined to give a rank k $\mathbb{F}_q$-linear set contained in $\mathcal{I}(\mathcal{C})$.

Sublines

Want to find $\mathbb{F}_q$ sublines contained in $\mathcal{I}(\mathcal{C})$ spanning a line external to $\mathcal{C}$, using the group of the conic we can fix an external line ℓ_e and a point $\boldsymbol{x}$, restrict our search for sublines of ℓ_e containing $\boldsymbol{x}$.



Subplanes and higher dimensional spaces

Looking for $\mathbb{F}_q$-subplanes in $\mathcal{I}(\mathcal{C})$, again restrict to subplanes containing $\boldsymbol{x}$.

We want **all** $\mathbb{F}_q$-sublines on $\boldsymbol{x}$, whether they span a secant or an external line to $\mathcal{C}$.

For each pair of sublines, generate points of their subplane one-by-one, check they are in $\mathcal{I}(\mathcal{C})$; if the test fails for a single point reject the pair as incompatible.

For ℓ occuring first in a compatible pair, define a graph on the sublines occuring second with adjacency given by compatibility.

A rank k $\mathbb{F}_q$-linear set will correspond to a $\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q - 1$ clique in such a graph, so we search for cliques of the appropriate size.

Subplanes and higher dimensional spaces

Looking for $\mathbb{F}_q$-subplanes in $\mathcal{I}(\mathcal{C})$, again restrict to subplanes containing $\boldsymbol{x}$.

We want **all** $\mathbb{F}_q$-sublines on $\boldsymbol{x}$, whether they span a secant or an external line to $\mathcal{C}$.

For each pair of sublines, generate points of their subplane one-by-one, check they are in $\mathcal{I}(\mathcal{C})$; if the test fails for a single point reject the pair as incompatible.

For ℓ occuring first in a compatible pair, define a graph on the sublines occuring second with adjacency given by compatibility.

A rank k $\mathbb{F}_q$-linear set will correspond to a $\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q - 1$ clique in such a graph, so we search for cliques of the appropriate size.

Subplanes and higher dimensional spaces

Looking for $\mathbb{F}_q$-subplanes in $\mathcal{I}(\mathcal{C})$, again restrict to subplanes containing $\boldsymbol{x}$.

We want **all** $\mathbb{F}_q$-sublines on $\boldsymbol{x}$, whether they span a secant or an external line to $\mathcal{C}$.

For each pair of sublines, generate points of their subplane one-by-one, check they are in $\mathcal{I}(\mathcal{C})$; if the test fails for a single point reject the pair as incompatible.

For ℓ occuring first in a compatible pair, define a graph on the sublines occuring second with adjacency given by compatibility.

A rank k $\mathbb{F}_q$-linear set will correspond to a $\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q - 1$ clique in such a graph, so we search for cliques of the appropriate size.

Subplanes and higher dimensional spaces

Looking for $\mathbb{F}_q$-subplanes in $\mathcal{I}(\mathcal{C})$, again restrict to subplanes containing $\boldsymbol{x}$.

We want **all** $\mathbb{F}_q$-sublines on $\boldsymbol{x}$, whether they span a secant or an external line to $\mathcal{C}$.

For each pair of sublines, generate points of their subplane one-by-one, check they are in $\mathcal{I}(\mathcal{C})$; if the test fails for a single point reject the pair as incompatible.

For ℓ occuring first in a compatible pair, define a graph on the sublines occuring second with adjacency given by compatibility.

A rank k $\mathbb{F}_q$-linear set will correspond to a $\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q - 1$ clique in such a graph, so we search for cliques of the appropriate size.

Subplanes and higher dimensional spaces

Looking for $\mathbb{F}_q$-subplanes in $\mathcal{I}(\mathcal{C})$, again restrict to subplanes containing $\boldsymbol{x}$.

We want **all** $\mathbb{F}_q$-sublines on $\boldsymbol{x}$, whether they span a secant or an external line to $\mathcal{C}$.

For each pair of sublines, generate points of their subplane one-by-one, check they are in $\mathcal{I}(\mathcal{C})$; if the test fails for a single point reject the pair as incompatible.

For ℓ occuring first in a compatible pair, define a graph on the sublines occuring second with adjacency given by compatibility.

A rank k $\mathbb{F}_q$-linear set will correspond to a $\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q - 1$ clique in such a graph, so we search for cliques of the appropriate size.

Results

	Number of sublines on $\boldsymbol{x} \in \ell_e$		
q	$n = 3$	$n = 4$	$n = 5$
3	12	120	1200
5	12	600	15072
7	24	912	52080
9	0	1040	91880
11	0	744	115572
13	0	504	102340
17	-	72	≥ 1
19	-	80	≥ 1
23	-	0	≥ 1
25	-	0	≥ 1
27	-	0	≥ 1
29	-	0	≥ 1
31	-	-	≥ 1

8-dimensional

An 8-dimensional R2CS is equivalent to a rank 4 linear set contained in $\mathcal{I}(\mathcal{C})$ for some conic $\mathcal{C}$ in $\mathrm{PG}(2, q^4)$.

While the bound tells us we could have $q < 30$, $q = 19$ is the largest value for which there is a suitable subline.

There are subplanes only when $q = 3$; have 237 graphs to test, the largest containing 204 vertices. Obtain 174 total cliques of size 12 all giving equivalent rank 4 linear sets (Cohen-Ganley R2CS).

Theorem

An 8-dimensional R2CS is either a Dickson semifield, or of Cohen–Ganley type (with center $\mathbb{F}_3$).

8-dimensional

An 8-dimensional R2CS is equivalent to a rank 4 linear set contained in $\mathcal{I}(\mathcal{C})$ for some conic $\mathcal{C}$ in $\mathrm{PG}(2, q^4)$.

While the bound tells us we could have $q < 30$, $q = 19$ is the largest value for which there is a suitable subline.

There are subplanes only when $q = 3$; have 237 graphs to test, the largest containing 204 vertices. Obtain 174 total cliques of size 12 all giving equivalent rank 4 linear sets (Cohen-Ganley R2CS).

Theorem

An 8-dimensional R2CS is either a Dickson semifield, or of Cohen–Ganley type (with center $\mathbb{F}_3$).

8-dimensional

An 8-dimensional R2CS is equivalent to a rank 4 linear set contained in $\mathcal{I}(\mathcal{C})$ for some conic $\mathcal{C}$ in $\mathrm{PG}(2, q^4)$.

While the bound tells us we could have $q < 30$, $q = 19$ is the largest value for which there is a suitable subline.

There are subplanes only when $q = 3$; have 237 graphs to test, the largest containing 204 vertices. Obtain 174 total cliques of size 12 all giving equivalent rank 4 linear sets (Cohen-Ganley R2CS).

Theorem

An 8-dimensional R2CS is either a Dickson semifield, or of Cohen–Ganley type (with center $\mathbb{F}_3$).

8-dimensional

An 8-dimensional R2CS is equivalent to a rank 4 linear set contained in $\mathcal{I}(\mathcal{C})$ for some conic $\mathcal{C}$ in $\mathrm{PG}(2, q^4)$.

While the bound tells us we could have $q < 30$, $q = 19$ is the largest value for which there is a suitable subline.

There are subplanes only when $q = 3$; have 237 graphs to test, the largest containing 204 vertices. Obtain 174 total cliques of size 12 all giving equivalent rank 4 linear sets (Cohen-Ganley R2CS).

Theorem

An 8-dimensional R2CS is either a Dickson semifield, or of Cohen–Ganley type (with center $\mathbb{F}_3$).

10-dimensional

Searching for suitable $\mathbb{F}_q$-linear sublines in $\mathrm{PG}(2, q^5)$ is more computationally difficult; as q starts to grow, we cannot search exhaustively.

We can complete the search for $q = 3$, finding two nonequivalent rank 5 linear sets (Cohen–Ganley and the Penttila–Williams examples).

Theorem

A 10-dimensional R2CS with center $\mathbb{F}_3$ is either a Dickson semifield, of Cohen–Ganley type, or Penttila–Williams.

10-dimensional

Searching for suitable $\mathbb{F}_q$-linear sublines in $\mathrm{PG}(2, q^5)$ is more computationally difficult; as q starts to grow, we cannot search exhaustively.

We can complete the search for $q = 3$, finding two nonequivalent rank 5 linear sets (Cohen–Ganley and the Penttila–Williams examples).

Theorem

A 10-dimensional R2CS with center $\mathbb{F}_3$ is either a Dickson semifield, of Cohen–Ganley type, or Penttila–Williams.

10-dimensional

Searching for suitable $\mathbb{F}_q$-linear sublines in $\mathrm{PG}(2, q^5)$ is more computationally difficult; as q starts to grow, we cannot search exhaustively.

We can complete the search for $q = 3$, finding two nonequivalent rank 5 linear sets (Cohen–Ganley and the Penttila–Williams examples).

Theorem

A 10-dimensional R2CS with center $\mathbb{F}_3$ is either a Dickson semifield, of Cohen–Ganley type, or Penttila–Williams.

Rank 3 commutative semifields

The situation for semifields having rank 3 over the left nucleus is more complicated.

For the case of semifields 6-dimensional over center $\mathbb{F}_q$, we need rank 6 $\mathbb{F}_q$-linear sets in $\mathrm{PG}(5, q^2)$ disjoint from the secant variety of the quadratic Veronesean $\mathcal{V}$.

There are no known examples of 6-dimensional R3CS when q is even. When q is odd, we have

- the twisted fields (Albert, 1961);
- the Budaghyan–Helleseth examples (2008);
- the Lunardon–Marino–Polverino–Trombetti examples (2011);
- the Zhou–Pott examples (2013).

Rank 3 commutative semifields

The situation for semifields having rank 3 over the left nucleus is more complicated.

For the case of semifields 6-dimensional over center $\mathbb{F}_q$, we need rank 6 $\mathbb{F}_q$-linear sets in $\mathrm{PG}(5, q^2)$ disjoint from the secant variety of the quadratic Veronesean $\mathcal{V}$.

There are no known examples of 6-dimensional R3CS when q is even. When q is odd, we have

- the twisted fields (Albert, 1961);
- the Budaghyan–Helleseth examples (2008);
- the Lunardon–Marino–Polverino–Trombetti examples (2011);
- the Zhou–Pott examples (2013).

Rank 3 commutative semifields

The situation for semifields having rank 3 over the left nucleus is more complicated.

For the case of semifields 6-dimensional over center $\mathbb{F}_q$, we need rank 6 $\mathbb{F}_q$-linear sets in $\mathrm{PG}(5, q^2)$ disjoint from the secant variety of the quadratic Veronesean $\mathcal{V}$.

There are no known examples of 6-dimensional R3CS when q is even. When q is odd, we have

- the twisted fields (Albert, 1961);
- the Budaghyan–Helleseth examples (2008);
- the Lunardon–Marino–Polverino–Trombetti examples (2011);
- the Zhou–Pott examples (2013).

Rank 3 commutative semifields

The situation for semifields having rank 3 over the left nucleus is more complicated.

For the case of semifields 6-dimensional over center $\mathbb{F}_q$, we need rank 6 $\mathbb{F}_q$-linear sets in $\mathrm{PG}(5, q^2)$ disjoint from the secant variety of the quadratic Veronesean $\mathcal{V}$.

There are no known examples of 6-dimensional R3CS when q is even. When q is odd, we have

- the twisted fields (Albert, 1961);
- the Budaghyan–Helleseth examples (2008);
- the Lunardon–Marino–Polverino–Trombetti examples (2011);
- the Zhou–Pott examples (2013).

Rank 3 commutative semifields

The situation for semifields having rank 3 over the left nucleus is more complicated.

For the case of semifields 6-dimensional over center $\mathbb{F}_q$, we need rank 6 $\mathbb{F}_q$-linear sets in $\mathrm{PG}(5, q^2)$ disjoint from the secant variety of the quadratic Veronesean $\mathcal{V}$.

There are no known examples of 6-dimensional R3CS when q is even. When q is odd, we have

- the twisted fields (Albert, 1961);
- the Budaghyan–Helleseth examples (2008);
- the Lunardon–Marino–Polverino–Trombetti examples (2011);
- the Zhou–Pott examples (2013).

Rank 3 commutative semifields

The situation for semifields having rank 3 over the left nucleus is more complicated.

For the case of semifields 6-dimensional over center $\mathbb{F}_q$, we need rank 6 $\mathbb{F}_q$-linear sets in $\mathrm{PG}(5, q^2)$ disjoint from the secant variety of the quadratic Veronesean $\mathcal{V}$.

There are no known examples of 6-dimensional R3CS when q is even. When q is odd, we have

- the twisted fields (Albert, 1961);
- the Budaghyan–Helleseth examples (2008);
- the Lunardon–Marino–Polverino–Trombetti examples (2011);
- the Zhou–Pott examples (2013).

Rank 3 commutative semifields

The situation for semifields having rank 3 over the left nucleus is more complicated.

For the case of semifields 6-dimensional over center $\mathbb{F}_q$, we need rank 6 $\mathbb{F}_q$-linear sets in $\mathrm{PG}(5, q^2)$ disjoint from the secant variety of the quadratic Veronesean $\mathcal{V}$.

There are no known examples of 6-dimensional R3CS when q is even. When q is odd, we have

- the twisted fields (Albert, 1961);
- the Budaghyan–Helleseth examples (2008);
- the Lunardon–Marino–Polverino–Trombetti examples (2011);
- the Zhou–Pott examples (2013).

A bound on q

Due to a recent result of Marino and Pepe (2016), we do have a bound on q.

They show that, when $q^2 > 2 \cdot 3^8$ (so $q > 114$) the list of R3CS from the previous slide is complete.

Furthermore, new examples for $q < 114$ must correspond to a $\mathbb{F}_q$-linear set consisting of $q^3 + q^2 + q + 1$ lines passing through a common point (a cone with base $\mathrm{PG}(3, q)$).

This restriction on the search space makes it more reasonable to search for examples (relatively; we only could do $q = 3$).

A bound on q

Due to a recent result of Marino and Pepe (2016), we do have a bound on q.

They show that, when $q^2 > 2 \cdot 3^8$ (so $q > 114$) the list of R3CS from the previous slide is complete.

Furthermore, new examples for $q < 114$ must correspond to a $\mathbb{F}_q$-linear set consisting of $q^3 + q^2 + q + 1$ lines passing through a common point (a cone with base $\mathrm{PG}(3, q)$).

This restriction on the search space makes it more reasonable to search for examples (relatively; we only could do $q = 3$).

A bound on q

Due to a recent result of Marino and Pepe (2016), we do have a bound on q.

They show that, when $q^2 > 2 \cdot 3^8$ (so $q > 114$) the list of R3CS from the previous slide is complete.

Furthermore, new examples for $q < 114$ must correspond to a $\mathbb{F}_q$-linear set consisting of $q^3 + q^2 + q + 1$ lines passing through a common point (a cone with base $\mathrm{PG}(3, q)$).

This restriction on the search space makes it more reasonable to search for examples (relatively; we only could do $q = 3$).

A bound on q

Due to a recent result of Marino and Pepe (2016), we do have a bound on q.

They show that, when $q^2 > 2 \cdot 3^8$ (so $q > 114$) the list of R3CS from the previous slide is complete.

Furthermore, new examples for $q < 114$ must correspond to a $\mathbb{F}_q$-linear set consisting of $q^3 + q^2 + q + 1$ lines passing through a common point (a cone with base $\mathrm{PG}(3, q)$).

This restriction on the search space makes it more reasonable to search for examples (relatively; we only could do $q = 3$).

Searching for linear sets

To extend our work on R2CS to the case of R3CS, we adapted our algorithms to the new setting of the quadratic Veronesean.

Searching for a suitable $\mathbb{F}_3$-linear set in $\mathrm{PG}(5,9)$, we worked in the quotient space wrt a point $\mathbf{x}$. Our task was then to find a rank 4 linear set (subgeometry) contained in a set $\mathcal{U}$ of "allowed" points.

We build such a set by adding a point at a time, forming a $\mathbb{F}_q$-basis for the linear set, and removing orbits of points from $\mathcal{U}$ as we went.

After a few months(!) of computer time:

Theorem

A 6-dimensional rank 3 commutative semifield with center $\mathbb{F}_3$ is isotopic to either a twisted field, or one of the examples given by BH, LMPT, ZP.

Searching for linear sets

To extend our work on R2CS to the case of R3CS, we adapted our algorithms to the new setting of the quadratic Veronesean.

Searching for a suitable $\mathbb{F}_3$-linear set in $\mathrm{PG}(5,9)$, we worked in the quotient space wrt a point $\mathbf{x}$. Our task was then to find a rank 4 linear set (subgeometry) contained in a set $\mathcal{U}$ of “allowed” points.

We build such a set by adding a point at a time, forming a $\mathbb{F}_q$-basis for the linear set, and removing orbits of points from $\mathcal{U}$ as we went.

After a few months(!) of computer time:

Theorem

A 6-dimensional rank 3 commutative semifield with center $\mathbb{F}_3$ is isotopic to either a twisted field, or one of the examples given by BH, LMPT, ZP.

Searching for linear sets

To extend our work on R2CS to the case of R3CS, we adapted our algorithms to the new setting of the quadratic Veronesean.

Searching for a suitable $\mathbb{F}_3$-linear set in $\mathrm{PG}(5,9)$, we worked in the quotient space wrt a point $\mathbf{x}$. Our task was then to find a rank 4 linear set (subgeometry) contained in a set $\mathcal{U}$ of "allowed" points.

We build such a set by adding a point at a time, forming a $\mathbb{F}_q$-basis for the linear set, and removing orbits of points from $\mathcal{U}$ as we went.

After a few months(!) of computer time:

Theorem

A 6-dimensional rank 3 commutative semifield with center $\mathbb{F}_3$ is isotopic to either a twisted field, or one of the examples given by BH, LMPT, ZP.

Searching for linear sets

To extend our work on R2CS to the case of R3CS, we adapted our algorithms to the new setting of the quadratic Veronesean.

Searching for a suitable $\mathbb{F}_3$-linear set in $\mathrm{PG}(5, 9)$, we worked in the quotient space wrt a point $\mathbf{x}$. Our task was then to find a rank 4 linear set (subgeometry) contained in a set $\mathcal{U}$ of "allowed" points.

We build such a set by adding a point at a time, forming a $\mathbb{F}_q$-basis for the linear set, and removing orbits of points from $\mathcal{U}$ as we went.

After a few months(!) of computer time:

Theorem

A 6-dimensional rank 3 commutative semifield with center $\mathbb{F}_3$ is isotopic to either a twisted field, or one of the examples given by BH, LMPT, ZP.

Searching for linear sets

To extend our work on R2CS to the case of R3CS, we adapted our algorithms to the new setting of the quadratic Veronesean.

Searching for a suitable $\mathbb{F}_3$-linear set in $\mathrm{PG}(5,9)$, we worked in the quotient space wrt a point $\mathbf{x}$. Our task was then to find a rank 4 linear set (subgeometry) contained in a set $\mathcal{U}$ of "allowed" points.

We build such a set by adding a point at a time, forming a $\mathbb{F}_q$-basis for the linear set, and removing orbits of points from $\mathcal{U}$ as we went.

After a few months(!) of computer time:

Theorem

A 6-dimensional rank 3 commutative semifield with center $\mathbb{F}_3$ is isotopic to either a twisted field, or one of the examples given by BH, LMPT, ZP.

Final remarks

Our techniques worked very well for classifying the 8-dimensional R2CS, but the 10-dimensional classification is much more difficult.

- Can we improve the bound on q in terms of n?
- Can we impose stronger structural requirements on the linear set $\mathcal{W}$?
- Is it even possible to have subplanes contained in $\mathcal{I}(\mathcal{C})$ when $q \not\equiv 0 \bmod 3$?

For R3CS, the clique-searching algorithm was completely impractical. We likely need better structural constraints (maybe on $\langle \mathcal{L} \rangle \cap \mathcal{V}$) to proceed.

Final remarks

Our techniques worked very well for classifying the 8-dimensional R2CS, but the 10-dimensional classification is much more difficult.

- Can we improve the bound on q in terms of n?
- Can we impose stronger structural requirements on the linear set $\mathcal{W}$?
- Is it even possible to have subplanes contained in $\mathcal{I}(\mathcal{C})$ when $q \not\equiv 0 \mod 3$?

For R3CS, the clique-searching algorithm was completely impractical. We likely need better structural constraints (maybe on $\langle \mathcal{L} \rangle \cap \mathcal{V}$) to proceed.

Final remarks

Our techniques worked very well for classifying the 8-dimensional R2CS, but the 10-dimensional classification is much more difficult.

- Can we improve the bound on q in terms of n?
- Can we impose stronger structural requirements on the linear set $\mathcal{W}$?
- Is it even possible to have subplanes contained in $\mathcal{I}(\mathcal{C})$ when $q \not\equiv 0 \bmod 3$?

For R3CS, the clique-searching algorithm was completely impractical. We likely need better structural constraints (maybe on $\langle \mathcal{L} \rangle \cap \mathcal{V}$) to proceed.

Final remarks

Our techniques worked very well for classifying the 8-dimensional R2CS, but the 10-dimensional classification is much more difficult.

- Can we improve the bound on q in terms of n?
- Can we impose stronger structural requirements on the linear set $\mathcal{W}$?
- Is it even possible to have subplanes contained in $\mathcal{I}(\mathcal{C})$ when $q \not\equiv 0 \bmod 3$?

For R3CS, the clique-searching algorithm was completely impractical. We likely need better structural constraints (maybe on $\langle \mathcal{L} \rangle \cap \mathcal{V}$) to proceed.

Final remarks

Our techniques worked very well for classifying the 8-dimensional R2CS, but the 10-dimensional classification is much more difficult.

- Can we improve the bound on q in terms of n?
- Can we impose stronger structural requirements on the linear set $\mathcal{W}$?
- Is it even possible to have subplanes contained in $\mathcal{I}(\mathcal{C})$ when $q \not\equiv 0 \bmod 3$?

For R3CS, the clique-searching algorithm was completely impractical. We likely need better structural constraints (maybe on $\langle \mathcal{L} \rangle \cap \mathcal{V}$) to proceed.