Commutative Semifields and the Equivalence Problem

Robert Coulter

Department of Mathematical Sciences
University of Delaware
Newark, DE 19716 USA
coulter@math.udel.edu

September 2014

The Basic Object

A finite *semifield* $\mathcal{R}$ is a finite algebraic system containing at least two elements, and possessing two binary operations, addition $+$ and multiplication $\star$, which satisfy the following axioms.

- $\langle \mathcal{R}, + \rangle$ is a group with identity 0.
- There are no zero divisors – if $a \star b = 0$, then $a = 0$ or $b = 0$.
- There is both a left and right distributive law –

$$a \star (b + c) = a \star b + a \star c$$
$$(a + b) \star c = a \star c + b \star c.$$

- There is unity $1 \in \mathcal{R}$ – $1 \star a = a \star 1 = a$.

The Basic Object

A finite *semifield* $\mathcal{R}$ is a finite algebraic system containing at least two elements, and possessing two binary operations, addition $+$ and multiplication $\star$, which satisfy the following axioms.

- $\langle \mathcal{R}, + \rangle$ is a group with identity 0.
- There are no zero divisors – if $a \star b = 0$, then $a = 0$ or $b = 0$.
- There is both a left and right distributive law –

$$a \star (b + c) = a \star b + a \star c$$
$$(a + b) \star c = a \star c + b \star c.$$

- There is unity $1 \in \mathcal{R}$ – $1 \star a = a \star 1 = a$.

If we do not insist upon the existence of unity, then we talk of a *presemifield*.

Immediate Observations

- Every field is a semifield; the term *proper semifield* means a semifield which is not a field – i.e. there exist elements a, b, c such that $(a \star b) \star c \neq a \star (b \star c)$.
- Existence of proper semifields was resolved in 1906 by Dickson, who constructed commutative examples of order q^2 for any $q = p^e$ with p odd and $e > 1$.
- It is easy to construct commutative presemifields which are not semifields – take any non-prime finite field $\mathbb{F}_q$ and any non-trivial automorphism σ of $\mathbb{F}_q$. Then the elements of $\mathbb{F}_q$, along with field addition and the multiplication $\star$ defined by $x \star y = (xy)^\sigma$ form a presemifield that does not have unity.

Immediate Implication

Theorem
The additive group of a presemifield $\mathcal{R}$ is elementary abelian.

Proof: Using the distributive laws in two ways we find

$$\begin{aligned}(a+b)\star(c+d) &= (a\star c + a\star d) + (b\star c + b\star d)\\ &= (a\star c + b\star c) + (a\star d + b\star d).\end{aligned}$$

Since $\langle \mathcal{R}, + \rangle$ is a group, we obtain $a\star d + b\star c = b\star c + a\star d$.
No zero divisors and finiteness together guarantee every element of $\mathcal{R}$ can be written as a product, and so $\langle \mathcal{R}, + \rangle$ is abelian.
To prove the elementary abelian part, one reverts to the classical argument proving the characteristic of a finite field is prime.

Immediate Implication of the Immediate Implication

Since $\langle \mathcal{R}, + \rangle$ is necessarily elementary abelian, the elements of $\mathcal{R}$ can be associated with the elements of a finite field $\mathbb{F}_q$ of the appropriate order.

Under this association, the multiplication $\star$ can be viewed as a bivariate function over $\mathbb{F}_q$ – i.e. $x \star y = M(x, y)$ for some bivariate polynomial $M \in \mathbb{F}_q[X, Y]$.

Moreover, interpolation, and the left and right distributive laws of $\mathcal{R}$, force M to take a very specific form:

$$x \star y = M(x, y) = \sum_{i,j=0}^{e-1} a_{ij} x^{p^i} y^{p^j},$$

where $q = p^e$.

Fields vs Semifields

Fields vs Semifields

Both algebraic structures must have prime power order and those of the same order have the same additive structure.

Fields vs Semifields

Both algebraic structures must have prime power order and those of the same order have the same additive structure.

BUT...

Fields vs Semifields

Both algebraic structures must have prime power order and those of the same order have the same additive structure.

BUT...

Finite fields were classified in the 1890s – there is exactly one, up to isomorphism, for each order.

Semifields are not classified – under isomorphism, there are many of each order – and we are not remotely close to classifying them, even under more appropriate forms of equivalence.

This last statement remains true even if we restrict ourselves to commutative semifields.

Fields vs Semifields

Both algebraic structures must have prime power order and those of the same order have the same additive structure.

BUT...

Finite fields were classified in the 1890s – there is exactly one, up to isomorphism, for each order.

Semifields are not classified – under isomorphism, there are many of each order – and we are not remotely close to classifying them, even under more appropriate forms of equivalence.

This last statement remains true even if we restrict ourselves to commutative semifields.

The Nuclei

Consider the following three subsets of a semifield $\mathcal{R} = (\mathbb{F}_q, +, \star)$:

$$\mathcal{N}_l(\mathcal{R}) = \{\alpha \in \mathcal{R} \ : \ (\alpha \star x) \star y = \alpha \star (x \star y) \text{ for all } x, y \in \mathcal{R}\}$$
$$\mathcal{N}_m(\mathcal{R}) = \{\alpha \in \mathcal{R} \ : \ (x \star \alpha) \star y = x \star (\alpha \star y) \text{ for all } x, y \in \mathcal{R}\}$$
$$\mathcal{N}_r(\mathcal{R}) = \{\alpha \in \mathcal{R} \ : \ (x \star y) \star \alpha = x \star (y \star \alpha) \text{ for all } x, y \in \mathcal{R}\}.$$

These are known as the left, middle and right nucleus, respectively. We also define

- the nucleus by $\mathcal{N} = \mathcal{N}_l \cap \mathcal{N}_m \cap \mathcal{N}_r$
- the weak nucleus $\mathcal{N}_w$ as the subset of $\mathcal{R}$ satisfying $(x \star y) \star z = x \star (y \star z)$ whenever any two of x, y, z are in $\mathcal{N}_w$.

It is easy to show all of these sets are finite fields.

Any semifield can be viewed as a vector space over its nucleus.

There be geometry here!

Given a presemifield $\mathcal{R} = \langle \mathcal{R}, +, \star \rangle$, you can define an affine plane $\mathcal{A}_\mathcal{R}$ in the following way:

- Points: $(x, y) \in \mathcal{R} \times \mathcal{R}$.
- Lines: $[m, b]$ and $[c]$, with $m, b, c \in \mathcal{R}$, defined by

$$[m, b] = \{(x, m \star x + b) : x \in \mathcal{R}\}$$
$$[c] = \{(c, y) : y \in \mathcal{R}\}.$$

The plane $\mathcal{A}_\mathcal{R}$, or its projective closure $\mathcal{P}_\mathcal{R}$, is called the *semifield plane coordinatised by* $\mathcal{R}$.

When $\mathcal{R} = \mathbb{F}_q$, one gets the Desarguesian plane.

Immediate obvious question

Given two semifields $\mathcal{R}_1$ and $\mathcal{R}_2$, when are $\mathcal{A}_1$ and $\mathcal{A}_2$ isomorphic?

It is sufficient, but not necessary, for $\mathcal{R}_1$ and $\mathcal{R}_2$ to be isomorphic in the ring-theoretical sense.

And this is the tip of the problem iceberg that is the equivalence problem.

Ring isomorphism turns out not to be the most suitable equivalence relation between semifields, at least in the geometric sense – you can have non-isomorphic semifields which coordinatise isomorphic planes.

Equivalence – Isotopism

Let $\mathcal{R}_1 = \langle \mathbb{F}_q, +, \star \rangle$ and $\mathcal{R}_2 = \langle \mathbb{F}_q, +, * \rangle$ be two presemifields.

Then $\mathcal{R}_1$ and $\mathcal{R}_2$ are isotopic if and only if there exists three non-singular linear transformations $L, M, N \in \mathbb{F}_q[X]$ such that

$$\forall x, y \in \mathbb{F}_q \ : \ M(x) \star N(y) = L(x * y).$$

We say that the triple (M, N, L) is an isotopism between $\mathcal{R}_1$ and $\mathcal{R}_2$.

Theorem (Albert)
Two presemifields coordinatise isomorphic planes if and only if they are isotopic.

How many?

Kantor's Conjecture

The number of pairwise non-isotopic presemifields of order q is not bounded above by a polynomial in q.

How many?

Kantor's Conjecture
The number of pairwise non-isotopic presemifields of order q is not bounded above by a polynomial in q.

Problem #1
Determine non-trivial bounds, lower or upper, for the number of pairwise non-isotopic presemifields of order q.

If you restrict the problem to characteristic 2, then Kantor has provided a suitable construction.

Planar functions

Let $f \in \mathbb{F}_q[X]$.

When q is odd, we say f is *planar* if for every $a \in \mathbb{F}_q^\star$, the difference/derivative polynomial $\Delta_{f,a}$ defined by

$$\Delta_{f,a}(X) = f(X + a) - f(X)$$

is a permutation polynomial.

Planar functions

Let $f \in \mathbb{F}_q[X]$.

When q is odd, we say f is *planar* if for every $a \in \mathbb{F}_q^\star$, the difference/derivative polynomial $\Delta_{f,a}$ defined by

$$\Delta_{f,a}(X) = f(X + a) - f(X)$$

is a permutation polynomial.

When q is even, we say f is *planar* if for every $a \in \mathbb{F}_q^\star$, the polynomial $\Delta'_{f,a}$ defined by

$$\Delta'_{f,a}(X) = f(X + a) - f(X) + aX$$

is a permutation polynomial.

DO polynomials...

Fix $q = p^e$, p a prime.

A polynomial $f \in \mathbb{F}_q[X]$ is a *Dembowski-Ostrom* (DO) polynomial if

$$f(X) = \sum_{i,j} a_{ij} X^{p^i + p^j}.$$

Also called "quadratic" in some circles.

Apart from one class of examples in characteristic 3, all known planar functions are DO polynomials – for characteristic at least 5, it is conjectured that DO polynomials are the only examples.

The Dembowski-Ostrom Conjecture

Problem #2

Prove there are no other non-DO polynomial examples of planar functions in odd characteristic.

The Dembowski-Ostrom Conjecture

Problem #2 – Coulter version
Prove there are no other non-DO polynomial examples of planar functions in odd characteristic.

The Dembowski-Ostrom Conjecture

Problem #2 – Coulter version
Prove there are no other non-DO polynomial examples of planar functions in odd characteristic.

Problem #2 – Pott version
Prove there are other non-DO polynomial examples of planar functions in odd characteristic.

The Dembowski-Ostrom Conjecture

Problem #2 – Coulter version pessimist
Prove there are no other non-DO polynomial examples of planar functions in odd characteristic.

Problem #2 – Pott version optimist
Prove there are other non-DO polynomial examples of planar functions in odd characteristic.

The Dembowski-Ostrom Conjecture

Problem #2 – Coulter version optimist
Prove there are no other non-DO polynomial examples of planar functions in odd characteristic.

Problem #2 – Pott version realist?
Prove there are other non-DO polynomial examples of planar functions in odd characteristic.

Commutative semifields and Planar DO polynomials

Fix $f \in \mathbb{F}_q[X]$ and define a "multiplication" $\star$ on $\mathbb{F}_q$ by

$$x \star y = f(x+y) - f(x) - f(y).$$

Theorem
The algebraic object $\mathcal{R}_f$ consisting of the elements of $\mathbb{F}_q$ along with field addition and the multiplication $\star$ is a commutative presemifield if and only if f is a planar DO polynomial.

Theorem
There is a one-to-one correspondence between commutative presemifields of odd order and (reduced) planar DO polynomials.

With a suitable tweak to the multiplication above, both of these results can be extended to characteristic 2.

Bilinear forms and Presemifields

A *bilinear form* B *on* $\mathbb{F}_q^n$ is a map from $\mathbb{F}_q^n \times \mathbb{F}_q^n$ to $\mathbb{F}_q$ satisfying

$$\begin{aligned} B(\mathbf{x}_1 + \mathbf{x}_2, \mathbf{y}) &= B(\mathbf{x}_1, \mathbf{y}) + B(\mathbf{x}_2, \mathbf{y}) \\ B(\mathbf{x}, \mathbf{y}_1 + \mathbf{y}_2) &= B(\mathbf{x}, \mathbf{y}_1) + B(\mathbf{x}, \mathbf{y}_2) \\ B(a\mathbf{x}, \mathbf{y}) &= B(\mathbf{x}, a\mathbf{y}) = aB(\mathbf{x},\mathbf{y}) \end{aligned}$$

for all $\mathbf{x}_i, \mathbf{y}_i \in \mathbb{F}_q^n$ and $a \in \mathbb{F}_q$.

Compare with a presemifield $\mathcal{R} = \langle \mathbb{F}_q, +, \star \rangle$ with nucleus $\mathcal{N}$, where we have

$$\begin{aligned} (x_1 + x_2) \star y &= x_1 \star y + x_2 \star y \\ x \star (y_1 + y_2) &= x \star y_1 + x \star y_2 \\ (ax) \star y &= x \star (ay) = a(x \star y) \end{aligned}$$

for all $x_i, y_i \in \mathbb{F}_q$ and $a \in \mathcal{N}$.

Quadratic forms and planar DO polynomials

A *quadratic form* Q *on* $\mathbb{F}_q^n$ is a map from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ satisfying

- $Q(a\mathbf{x}) = a^2 Q(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{F}_q^n$ and $a \in \mathbb{F}_q$.
- $B(\mathbf{x}, \mathbf{y}) = Q(\mathbf{x} + \mathbf{y}) - Q(\mathbf{x}) - Q(\mathbf{y})$ is a symmetric bilinear form.

Compare with a planar DO polynomial

$$f(X) = \sum a_{ij} X^{p^i + p^j} \in \mathbb{F}_q[X]:$$

- $f(ax) = a^2 f(x)$ for all $x \in \mathbb{F}_q$ and $a \in \mathbb{F}_p$.
- $x \star y = f(x + y) - f(x) - f(y)$ is the multiplication of a commutative presemifield.

So close

Problem #3
Can a reasonable theory be developed for the commutative semifield/planar DO polynomial duality along similar lines to the bilinear form/quadratic form duality?

More specifically, can any of the enumeration techniques developed for counting inequivalent forms be adapted to obtain non-trivial bounds for the number of inequivalent commutative semifields? (see Problem #1)

The MAIN problem with the theory

Problem #4
Classify presemifields.

The MAIN problem with the theory

Problem #4
Classify presemifields.

If that's too hard, classify commutative presemifields.

The MAIN problem with the theory

Problem #4
Classify presemifields.

If that's too hard, classify commutative presemifields.

If that's too hard...

The MAIN problem with the theory

Problem #4
Classify presemifields.

If that's too hard, classify commutative presemifields.

If that's too hard... maybe find an intelligent person to help?

The MAIN problem with the theory

Problem #4
Classify presemifields.

If that's too hard, classify commutative presemifields.

If that's too hard. . . maybe find an intelligent person to help?
Or even a whole room full of them?

The MAIN problem with the theory

Problem #4
Classify presemifields.

If that's too hard, classify commutative presemifields.

If that's too hard... maybe find an intelligent person to help?
Or even a whole room full of them?

The situation is not completely hopeless – orders p, p^2 and p^3 are done.

Isotopism for Commutative presemifields

Let $\mathcal{R}_1 = \langle \mathbb{F}_q, +, \star \rangle$ and $\mathcal{R}_2 = \langle \mathbb{F}_q, +, * \rangle$ be two commutative presemifields.

Then $\mathcal{R}_1$ and $\mathcal{R}_2$ are isotopic if and only if there exists three non-singular linear transformations $L, M, N \in \mathbb{F}_q[X]$ such that, for all $x, y \in \mathbb{F}_q$, we have

$$M(x) \star N(y) = L(x * y)$$

Isotopism for Commutative presemifields

Let $\mathcal{R}_1 = \langle \mathbb{F}_q, +, \star \rangle$ and $\mathcal{R}_2 = \langle \mathbb{F}_q, +, * \rangle$ be two commutative presemifields.

Then $\mathcal{R}_1$ and $\mathcal{R}_2$ are isotopic if and only if there exists three non-singular linear transformations $L, M, N \in \mathbb{F}_q[X]$ such that, for all $x, y \in \mathbb{F}_q$, we have

$$M(x) \star N(y) = L(x * y) = L(y * x) = M(y) \star N(x).$$

Isotopism for Commutative presemifields

Let $\mathcal{R}_1 = \langle \mathbb{F}_q, +, \star \rangle$ and $\mathcal{R}_2 = \langle \mathbb{F}_q, +, * \rangle$ be two commutative presemifields.

Then $\mathcal{R}_1$ and $\mathcal{R}_2$ are isotopic if and only if there exists three non-singular linear transformations $L, M, N \in \mathbb{F}_q[X]$ such that, for all $x, y \in \mathbb{F}_q$, we have

$$M(x) \star N(y) = L(x * y) = L(y * x) = M(y) \star N(x).$$

Is it reasonable to expect that, in the case of commutative presemifields, isotopism implies strong isotopism (i.e. $M = N$)?

Not quite Reasonable, but still Respectable

Theorem

Let $\mathcal{R}_1 = \langle \mathbb{F}_q, +, \star \rangle$ and $\mathcal{R}_2 = \langle \mathbb{F}_q, +, * \rangle$ be isotopic commutative semifields with $d = [\mathcal{N}_m : \mathcal{N}]$ the dimension of the middle nucleus over the nucleus.

- If d is odd, then $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic.
- If d is even, then either $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic or the only isotopisms between them are of the form $(\alpha \star N, N, L)$ where α is a non-square element of $\mathcal{N}_m(\mathcal{R}_1)$.

In particular, if $q = p^e$ with $p = 2$ or e odd, then $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic.

The result can be extended to commutative presemifields.

Limitations of the Second Part of the Theorem

If d is even, then either $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic or the only isotopisms between them are of the form $(\alpha \star N, N, L)$ where α is a non-square element of $\mathcal{N}_m(\mathcal{R}_1)$.

Limitations of the Second Part of the Theorem

If d is even, then either $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic or the only isotopisms between them are of the form $(\alpha \star N, N, L)$ where α is a non-square element of $\mathcal{N}_m(\mathcal{R}_1)$.

The 2nd possibility does occur – examples are known for order 3^8, the smallest possibility.

When it does, the isotopy class containing $\mathcal{R}_1$ and $\mathcal{R}_2$ splits into exactly two strong isotopy classes.

Thus the number of pairwise non-isotopic commutative presemifields of order q is less than 2 times the number of pairwise non-strongly isotopic commutative presemifields.

Another problem...

This splitting of isotopism classes is not well understood.

Problem #5
Find a key property or an efficient test that determines when the isotopy class of a given commutative presemifield splits into two strong isotopy classes.

Another problem...

This splitting of isotopism classes is not well understood.

Problem #5
Find a key property or an efficient test that determines when the isotopy class of a given commutative presemifield splits into two strong isotopy classes.

Maybe not hard? I know of no work done on trying to tie this down.

Strong Isotopy via Planar DO polynomials

Now let $\mathcal{R}_f$ and $\mathcal{R}_h$ be two commutative presemifields generated by planar DO polynomials $f, h \in \mathbb{F}_q[X]$, respectively.

Theorem
$\mathcal{R}_f$ and $\mathcal{R}_h$ are strongly isotopic, with strong isotopy (M, M, L), if and only if

$$L(f(X)) \equiv h(M(X)) \pmod{X^q - X}.$$

The similarity with EA-equivalence will be immediately apparent to everyone here.

Strong Isotopy via Planar DO polynomials

Now let $\mathcal{R}_f$ and $\mathcal{R}_h$ be two commutative presemifields generated by planar DO polynomials $f, h \in \mathbb{F}_q[X]$, respectively.

Theorem
$\mathcal{R}_f$ and $\mathcal{R}_h$ are strongly isotopic, with strong isotopy (M, M, L), if and only if

$$L(f(X)) \equiv h(M(X)) \pmod{X^q - X}.$$

The similarity with EA-equivalence will be immediately apparent to everyone here.

The inherent difficulties with using the equivalence relation are also similar!

More Problems

Problem #6

Find some technique from the use of EA-equivalence on boolean functions that can be exploited to obtain some sort of result on the numbers of non-isotopic commutative presemifields.

More Problems

Problem #6

Find some technique from the use of EA-equivalence on boolean functions that can be exploited to obtain some sort of result on the numbers of non-isotopic commutative presemifields.

Hard, and (it must be acknowledged) some of you here have already tried this!

More Problems – I have many!

Problem #6

Find some technique from the use of EA-equivalence on boolean functions that can be exploited to obtain some sort of result on the numbers of non-isotopic commutative presemifields.

Hard, and (it must be acknowledged) some of you here have already tried this!

Problem #7

Find a better way to resolve the equivalence issue, possibly even through the introduction of a new equivalence relation.

More Problems – I have many!

Problem #6

Find some technique from the use of EA-equivalence on boolean functions that can be exploited to obtain some sort of result on the numbers of non-isotopic commutative presemifields.

Hard, and (it must be acknowledged) some of you here have already tried this!

Problem #7

Find a better way to resolve the equivalence issue, possibly even through the introduction of a new equivalence relation.

Hard; there may not even be one! One can try CCZ-equivalence, but as with EA-equivalence, similar difficulties arise.

One Approach – restrict the form

Theorem (odd characteristic p only)
Let e, k, d be natural numbers with $ek = 1$ and $d = 2$ or $ek > 1$ and d arbitrary.
Set $s = p^e$, $v = r^k$, $q = v^d$ and $t(X) = X^v - X$.
If $\mathcal{R}$ is a commutative semifield with $\mathbb{F}_s \subseteq \mathcal{N}$ and $\mathbb{F}_v \subseteq \mathcal{N}_w$, then $\mathcal{R} \approx \mathcal{R}_f$ where f is a planar DO polynomial of the form

$$f(X) = L(t^2(X)) + D(t(X)) + \frac{1}{2}X^2$$

with $L \in \mathbb{F}_q[X]$ a s-polynomial and $D \in \mathbb{F}_q[X]$ a DO polynomial of a specific form.

Restrictions lead to restrictions

When dealing exclusively with planar DO polynomials of the form

$$L(t^2(X)) + D(t(X)) + \frac{1}{2}X^2,$$

isotopic examples must be connected via isotopisms of restricted form too – i.e. the shape of the non-singular transformations involved are dependent on the $\mathcal{N}$ and $\mathcal{N}_w$ also.

Restrictions lead to restrictions, but not enough restrictions

When dealing exclusively with planar DO polynomials of the form

$$L(t^2(X)) + D(t(X)) + \frac{1}{2}X^2,$$

isotopic examples must be connected via isotopisms of restricted form too – i.e. the shape of the non-singular transformations involved are dependent on the $\mathcal{N}$ and $\mathcal{N}_w$ also.

We have had little success with this approach, though it might be strong enough to deal with p^4 order, when $D(X) = 0$ is forced.

Restrictions lead to restrictions, but not enough restrictions

When dealing exclusively with planar DO polynomials of the form

$$L(t^2(X)) + D(t(X)) + \frac{1}{2}X^2,$$

isotopic examples must be connected via isotopisms of restricted form too – i.e. the shape of the non-singular transformations involved are dependent on the $\mathcal{N}$ and $\mathcal{N}_w$ also.

We have had little success with this approach, though it might be strong enough to deal with p^4 order, when $D(X) = 0$ is forced.

Problem #8

Find other, more useful, restrictions on the forms of planar DO polynomials which can be used to study all commutative semifields of specified type.

A Second Approach – illustrated by a specific example...

Theorem

For any non-zero $a \in \mathbb{F}_{3^e}$, the polynomial

$$f_a(X) = X^{10} + aX^6 - a^2X^2$$

is a planar DO polynomial over $\mathbb{F}_{3^e}$ if and only if

- e is odd, or
- $e = 2$ and $a = \pm 1$.

Further, for $e \geq 3$ odd, $f_a(X)$ and $f_b(X)$ generate isotopic commutative presemifields if and only if ab is a square.

An example with a quirk

Now fix $e \geq 3$ odd, set $q = 3^e$ and choose $a, b \in \mathbb{F}_q$ so that ab is a non-square.

- Then $f_a(X)$ and $f_b(X)$ are not isotopic – in practical terms, for all linearized permutation polynomials $L, M \in \mathbb{F}_q[X]$, we have

$$L(f_a(X)) \not\equiv f_b(M(X)) \pmod{X^q - X}.$$

An example with a quirk

Now fix $e \geq 3$ odd, set $q = 3^e$ and choose $a, b \in \mathbb{F}_q$ so that ab is a non-square.

- Then $f_a(X)$ and $f_b(X)$ are not isotopic – in practical terms, for all linearized permutation polynomials $L, M \in \mathbb{F}_q[X]$, we have

$$L(f_a(X)) \not\equiv f_b(M(X)) \pmod{X^q - X}.$$

- Over $\mathbb{F}_{q^2}$ we do not get presemifields – there are zero divisors – but the polynomials are *strongly isotopic via linear polynomials*:

$$d^{10} f_a(X) = f_b(dx),$$

where $d \in \mathbb{F}_{q^2}$ satisfies $d^4 = ba^{-1}$.

Two Final Problems

Problem #9

What does this relationship mean for the respective commutative semifields?

Is there a deeper relation between the two affine planes than presently understood?

Are there other examples of this phenomena, either within the study of commutative semifields, or in similar fields (APN functions come to mind) and can they be classified?

Problem #10

Does this relationship point towards some generalisation of the equivalence relation which can be handled more neatly than current techniques?

I'm done.

Thank you.