Equivalences and symmetries in combinatorial structures: From Boolean functions to finite geometries

Lukas Kölsch

University of South Florida

(all original work is joint work with Faruk Göloğlu)

Basics

Equivalences and symmetries are studied for combinatorial and algebraic structures - designs, codes, projective planes, fields, curves...

For Boolean functions equivalence has a special significance since many cryptographic properties are invariant under certain equivalences.

Basics

In this talk: "Boolean functions" are vectorial p-ary Boolean functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

(everything more or less translates to the general case $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$)

What is the "correct" notion of equivalence for Boolean functions? It should preserve all essential properties while being as general as possible.

Equivalence

Definition

We call two functions $F, G\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ *equivalent* if there is an $A \in \mathrm{AGL}(\mathbb{F}_{p^n}^2)$ such that

$$A(\Gamma_F) = \Gamma_G$$

where $\Gamma_F = \{(x, F(x))^t : x \in \mathbb{F}_{p^n}\}$ is the graph of a function.

We write $F \sim G$.

This notion of equivalence preserves most interesting properties of the function that are important for cryptography.

Equivalence - special cases

If F, G are equivalent via $A = \begin{pmatrix} A_1 & 0 \\ A_3 & A_4 \end{pmatrix}$:

This means $G(A_1(x)) = F(A_4(x)) + A_3(x)$.

Every bijective function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is equivalent to its inverse by choosing $A = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$.

Automorphisms/Symmetries

Definition

We denote by $\mathrm{Aut}(F)$ the automorphism group of F, i.e.

$$\mathrm{Aut}(F) = \{A \in \mathrm{AGL}(\mathbb{F}_{p^n}^2) \colon A(\Gamma_F) = \Gamma_F\}$$

We can think of automorphisms as symmetries of F.

If we view this as a group action: $\mathrm{AGL}(\mathbb{F}_{p^n}^2)$ acting on $\mathbb{F}_{p^n}^2$.

Γ_F and Γ_G are in the same orbit $\Leftrightarrow$ F, G are equivalent.

$A \in \mathrm{Aut}(F) \Leftrightarrow A$ is in the stabilizer of Γ_F.

Checking equivalence in practice

For specific functions F, G inequivalence can be checked by computer, usually via invariants.

However, this becomes infeasible fast!

Generally, it is desirable to have mathematical proofs instead, in particular for certain classes/families of functions!

Equivalence via automorphism group

It helps to look at automorphisms!

Lemma

Let $F \sim G$. Then there is $\gamma \in \mathrm{AGL}(\mathbb{F}_{p^n}^2)$ such that

$$\mathrm{Aut}(F) = \gamma^{-1} \mathrm{Aut}(G)\gamma.$$

So equivalent functions have conjugate automorphism groups!

However, computing the automorphism group is very hard usually!

Idea: Do not compute entire automorphism group, but only a sufficiently big part.

Power functions

Let us look at the most simple functions: power functions
$F, G\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $F(x) = x^{d_1}$, $G(x) = x^{d_2}$.

Question

When are F, G equivalent?

There are obvious equivalences: $F \sim G$ if $d_2 \equiv p^i d_1 \pmod{p^n - 1}$ or $d_2 d_1 \equiv p^i \pmod{p^n - 1}$.

But are there more equivalences? We look at the automorphism groups!

Power functions

Let us find some automorphisms of $F(x) = x^d$:

We clearly have $F(ax) = a^d F(x)$ (since $(ax)^d = a^d x^d$) for any $a \in \mathbb{F}_{p^n}^\times$.

Power functions

Let us find some automorphisms of $F(x) = x^d$:

We clearly have $F(ax) = a^d F(x)$ (since $(ax)^d = a^d x^d$) for any $a \in \mathbb{F}_{p^n}^\times$.

So $A = \left(\begin{smallmatrix} a & 0 \\ 0 & a^d \end{smallmatrix}\right) \in \mathrm{Aut}(F)$, since

$$\begin{pmatrix} a & 0 \\ 0 & a^d \end{pmatrix} \begin{pmatrix} x \\ F(x) \end{pmatrix} = \begin{pmatrix} ax \\ a^d F(x) \end{pmatrix}$$

and $\left\{ \begin{pmatrix} ax \\ a^d F(x) \end{pmatrix} : x \in \mathbb{F}_{p^n} \right\} = \Gamma_F$

via $x \mapsto x/a$.

Power functions

Let us find some automorphisms of $F(x) = x^d$:

We clearly have $F(ax) = a^d F(x)$ (since $(ax)^d = a^d x^d$) for any $a \in \mathbb{F}_{p^n}^\times$.

So $A = \left(\begin{smallmatrix} a & 0 \\ 0 & a^d \end{smallmatrix}\right) \in \mathrm{Aut}(F)$, since

$$\begin{pmatrix} a & 0 \\ 0 & a^d \end{pmatrix} \begin{pmatrix} x \\ F(x) \end{pmatrix} = \begin{pmatrix} ax \\ a^d F(x) \end{pmatrix}$$

and $\left\{ \begin{pmatrix} ax \\ a^d F(x) \end{pmatrix} : x \in \mathbb{F}_{p^n} \right\} = \Gamma_F$

via $x \mapsto x/a$.

So $A^{(d)} = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & a^d \end{smallmatrix}\right) : a \in \mathbb{F}_{p^n}^\times \right\}$ is a cyclic subgroup of $\mathrm{Aut}(F)$ with $p^n - 1$ elements.

Equivalence via automorphism group

Lemma

Let $F \sim G$. Then there is $\gamma \in \mathrm{AGL}(\mathbb{F}_{p^n}^2)$ such that

$$\mathrm{Aut}(F) = \gamma^{-1} \mathrm{Aut}(G)\gamma.$$

$F(x) = x^{d_1}$, $G(x) = x^{d_2}$ both have these big subgroups $A^{(d_1)}$, $A^{(d_2)}$ in their automorphism groups *of the same order* $p^n - 1$.

Equivalence via automorphism group

Lemma

Let $F \sim G$. Then there is $\gamma \in \mathrm{AGL}(\mathbb{F}_{p^n}^2)$ such that

$$\mathrm{Aut}(F) = \gamma^{-1} \mathrm{Aut}(G)\gamma.$$

$F(x) = x^{d_1}$, $G(x) = x^{d_2}$ both have these big subgroups $A^{(d_1)}$, $A^{(d_2)}$ in their automorphism groups *of the same order* $p^n - 1$.

Rough proof idea: Prove that if $\mathrm{Aut}(F)$ and $\mathrm{Aut}(G)$ are conjugate then $A^{(d_1)}$ and $A^{(d_2)}$ are conjugate. (Hard part!)
$A^{(d_1)}$ and $A^{(d_2)}$ have simple structure such that the conjugation can be calculated easily.

This is the proof idea followed by Yoshiara (special cases) and Dempwolff (general case).

Theorem (Dempwolff, 2016)

Let $F(x) = x^{d_1}$, $G(x) = x^{d_2}$ be power functions on $\mathbb{F}_{p^n}$. $F \sim G$ if and only if $d_2 \equiv p^i d_1 \pmod{p^n - 1}$ or $d_2 d_1 \equiv p^i \pmod{p^n - 1}$ for some i.

What happened?

They used the nice structure of the power functions (nice subgroups in the automorphism group) to prove inequivalence.

The same idea works (with modifications) also for other families that have strong symmetries!

Example

Let $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ be a function defined via

$$F(x, y) = (F_1(x, y), F_2(x, y))$$

where $F_1, F_2 : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ are homogeneous polynomials of degree $q + 1$ (resp. $r + 1$) where q, r are powers of p.

Göloğlu was the first to systematically investigate these functions and discovered the importance of this structure. He called them *biprojective functions*.

APN and planar functions

The reason Göloğlu investigated these functions is that many APN functions have this structure. Later it also appeared that the same is true for planar functions.

Definition

Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. If $D_{a,F}(x) = F(x+a) - F(x) = b$ has 1 solution for $a \in \mathbb{F}_{p^n}^{\times}$, $b \in \mathbb{F}_{p^n}$ we call F planar. If it has at most 2 solution, we call it almost perfect nonlinear (APN).

Planar functions exist only in odd characteristic, APN functions are mostly interesting in even characteristic because of good properties used in cryptography.

APN and planar functions

The reason Göloğlu investigated these functions is that many APN functions have this structure. Later it also appeared that the same is true for planar functions.

However, often this structure was "hidden".

Example (Zhou-Pott, 2011)

$$F(x,y) = (xy, x^{q+1} + d(y^{q+1})^r),$$

where $q = 2^k, r = 2^j$, m even, $\gcd(k,m) = 1$ and some condition on d.

...is equivalent to...

$$F(x,y) = (x^{q+1} + dy^{q+1}, xy^r).$$

Examples of biprojective APN functions over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$:

Example (Carlet, 2010)

$$F(x, y) = (xy, x^{q+1} + bxy^q + ay^{q+1}),$$

where $q = 2^k$, $\gcd(k, m) = 1$ and $P = x^{q+1} + bx + a$ has no roots in $\mathbb{F}_{2^m}$.

Example (Taniguchi, 2018)

$$F(x, y) = (xy, x^{q^2+q^3} + bx^{q^2}y^{q^2} + ay^{q+1}),$$

where $q = 2^k$, $\gcd(k, m) = 1$ and $P = x^{q+1} + bx + a$ has no roots in $\mathbb{F}_{2^m}$.

...is equivalent to...

$$F(x, y) = (x^{q+1} + bxy^q + ay^{q+1}, xy^{q^2}).$$

Example (Göloğlu, K., 2021)

$$F(x,y) = (x^{q+1} + by^{q+1}, x^r y + (a/b)xy^r),$$

where $q = 2^k$,$r = 2^{k+m/2}$, m even, $\gcd(k,m) = 1$, $a \in \mathbb{F}_{2^{m/2}}^{\times}$, b a non-square in $\mathbb{F}_{p^m}$.

and others (Göloğlu, Gold).

The same is also true for planar functions (Dickson, Budaghyan-Helleseth, Göloğlu-K.,. . .)

Why is this "biprojective" setting useful?

It helps with two obvious questions:

Question

Are the different families (partly) equivalent? Are they completely distinct (i.e. don't intersect at all)?

Question

How big are the families, i.e. which choice of parameters yields equivalent/inequivalent functions?

Both questions are generally very hard - but in this case feasible because of the special structure!

Finding automorphisms of biprojective functions

We are interested in functions defined via

$$F(x, y) = (F_1(x, y), F_2(x, y))$$

where $F_1, F_2 \colon \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ are homogeneous polynomials of degree $q + 1$ (resp. $r + 1$) where q, r are powers of p.

Set $A = \left(\begin{smallmatrix} A_1 & 0 \\ 0 & A_4 \end{smallmatrix}\right)$ via $A_1 = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ and $A_4 = \left(\begin{smallmatrix} a^{q+1} & 0 \\ 0 & a^{r+1} \end{smallmatrix}\right)$.
Then

$$F(A_1(x, y)) = (a^{q+1} F_1(x, y), a^{r+1} F_2(x, y)) = A_4(F(x, y)).$$

So A is an automorphism for any $a \in \mathbb{F}_{p^m}^{\times}$.

$\implies$ Biprojective functions always have a cyclic subgroup in their automorphism group of order $p^m - 1$.

Finding automorphisms of biprojective functions

Biprojective functions always have a cyclic subgroup in their automorphism group of order $p^m - 1$!

This is very similar to the big subgroup in the power functions case!

So we attempted to get a Yoshiara-Dempwolff style proof. But things are much more involved because power functions are much simpler.

We had to adapt the techniques considerably...

Show that two biprojective functions F_1, F_2 are not equivalent - in five simple steps!

Show that two biprojective functions F_1, F_2 are not equivalent - in five simple steps!

- Let $H_1 \leq \mathrm{Aut}(F_1)$, $H_2 \leq \mathrm{Aut}(F_2)$ with $|H_1| = |H_2| = p^m - 1$ be the nice cyclic automorphism subgroups.

Show that two biprojective functions F_1, F_2 are not equivalent - in five simple steps!

- Let $H_1 \leq \mathrm{Aut}(F_1)$, $H_2 \leq \mathrm{Aut}(F_2)$ with $|H_1| = |H_2| = p^m - 1$ be the nice cyclic automorphism subgroups.
- Choose a suitable prime p' and Sylow p'-groups $S_1 \leq H_1$, $S_2 \leq H_2$.

Show that two biprojective functions F_1, F_2 are not equivalent - in five simple steps!

- Let $H_1 \leq \mathrm{Aut}(F_1)$, $H_2 \leq \mathrm{Aut}(F_2)$ with $|H_1| = |H_2| = p^m - 1$ be the nice cyclic automorphism subgroups.
- Choose a suitable prime p' and Sylow p'-groups $S_1 \leq H_1$, $S_2 \leq H_2$.
- Prove that S_1, S_2 are also Sylow p'-groups of $\mathrm{Aut}(F_1), \mathrm{Aut}(F_2)$ (key step!)

Show that two biprojective functions F_1, F_2 are not equivalent - in five simple steps!

- Let $H_1 \leq \mathrm{Aut}(F_1)$, $H_2 \leq \mathrm{Aut}(F_2)$ with $|H_1| = |H_2| = p^m - 1$ be the nice cyclic automorphism subgroups.
- Choose a suitable prime p' and Sylow p'-groups $S_1 \leq H_1$, $S_2 \leq H_2$.
- Prove that S_1, S_2 are also Sylow p'-groups of $\mathrm{Aut}(F_1), \mathrm{Aut}(F_2)$ (key step!)
- If $\gamma^{-1}\,\mathrm{Aut}(F_1)\gamma = \mathrm{Aut}(F_2)$ then $\gamma^{-1}S_1\gamma$ is a Sylow subgroup of $\mathrm{Aut}(F_2)$. So $\gamma^{-1}S_1\gamma$ and S_2 are conjugate in $\mathrm{Aut}(F_2)$ (by Sylow's theorem)!

Show that two biprojective functions F_1, F_2 are not equivalent - in five simple steps!

- Let $H_1 \leq \mathrm{Aut}(F_1)$, $H_2 \leq \mathrm{Aut}(F_2)$ with $|H_1| = |H_2| = p^m - 1$ be the nice cyclic automorphism subgroups.
- Choose a suitable prime p' and Sylow p'-groups $S_1 \leq H_1$, $S_2 \leq H_2$.
- Prove that S_1, S_2 are also Sylow p'-groups of $\mathrm{Aut}(F_1), \mathrm{Aut}(F_2)$ (key step!)
- If $\gamma^{-1}\,\mathrm{Aut}(F_1)\gamma = \mathrm{Aut}(F_2)$ then $\gamma^{-1}S_1\gamma$ is a Sylow subgroup of $\mathrm{Aut}(F_2)$. So $\gamma^{-1}S_1\gamma$ and S_2 are conjugate in $\mathrm{Aut}(F_2)$ (by Sylow's theorem)!
- Determine all $\delta \in \mathrm{AGL}(\mathbb{F}_{p^n}^2)$ such that $\delta^{-1}S_1\delta = S_2$. If all $\delta \notin \mathrm{Aut}(F_2)$ then F_1, F_2 are not equivalent

In some sense, checking $\gamma^{-1}\,\mathrm{Aut}(F_1)\gamma = \mathrm{Aut}(F_2)$ is reduced to checking $\delta^{-1}S_1\delta = S_2$.

Prove that S_1 is also Sylow p'-groups of $\mathrm{Aut}(F_1), \mathrm{Aut}(F_2)$ (key step!)

Prove that S_1 is also Sylow p'-groups of $\mathrm{Aut}(F_1), \mathrm{Aut}(F_2)$ (key step!)

Reduce the problem from $\mathrm{AGL}(\mathbb{F}_{p^n}^2)$ to $\mathrm{GL}(\mathbb{F}_{p^n}^2)$.

Prove that all Sylow p'-groups of $\mathrm{GL}(\mathbb{F}_{p^n}^2)$ are abelian.

Let T be a Sylow p'-group of $\mathrm{GL}(\mathbb{F}_{p^n}^2)$ containing S_1.

It must be contained in the centralizer

$$C_{\mathrm{GL}(\mathbb{F}_{p^n}^2)}(S_1) = \{x \in \mathrm{GL}(\mathbb{F}_{p^n}^2) \colon xg = gx \text{ for all } g \in S_1\}.$$

Compute this centralizer and hope that $p' \nmid [C_{\mathrm{GL}\,\mathbb{F}_{p^n}^2} : S_1]$.

Then $T = S_1$.

Prove that S_1 is also Sylow p'-groups of $\mathrm{Aut}(F_1), \mathrm{Aut}(F_2)$ (key step!)

Reduce the problem from $\mathrm{AGL}(\mathbb{F}_{p^n}^2)$ to $\mathrm{GL}(\mathbb{F}_{p^n}^2)$.

Prove that all Sylow p'-groups of $\mathrm{GL}(\mathbb{F}_{p^n}^2)$ are abelian.

Let T be a Sylow p'-group of $\mathrm{GL}(\mathbb{F}_{p^n}^2)$ containing S_1.

It must be contained in the centralizer

$$C_{\mathrm{GL}(\mathbb{F}_{p^n}^2)}(S_1) = \{x \in \mathrm{GL}(\mathbb{F}_{p^n}^2) \colon xg = gx \text{ for all } g \in S_1\}.$$

Compute this centralizer and hope that $p' \nmid [C_{\mathrm{GL}\,\mathbb{F}_{p^n}^2} : S_1]$.

Then $T = S_1$.

(what if $p' \mid [C_{\mathrm{GL}(\mathbb{F}_{p^n}^2)}(S_1) \colon S_1]$? Iterate the process with the new subgroup.)

We can apply this technique to all biprojective APN functions and get complete results on the equivalences!

- We show that all known biprojective APN families are disjoint (except some simple edge cases)

- We precisely determine how many inequivalent functions each APN family contains

-In particular, we prove that the new family we found is (together with the Taniguchi APN family) the only family known so far that yields exponentially many (in the dimension n) APN functions

What's next?

So this inequivalence technique works for power functions and biprojective functions. What's next?

In order for the technique to work, one needs a simple and large subgroup in the autormorphism group!

It is currently unclear to us how "rare" this is for APN functions.

But automorphism groups seem to be a key and should always be investigated!

Some ideas of questions regarding automorphism groups

It is hopeless to classify all APN functions - but are partial results possible?

Question

Let F be an APN function on $\mathbb{F}_{2^n}$ with a cyclic subgroup of order $p^n - 1$ in its automorphism group. Is F equivalent to a power function?

Question

Let F be an APN function on $\mathbb{F}_{2^{2m}}$ with a cyclic subgroup of order $p^m - 1$ in its automorphism group. Is F equivalent to a power function or a biprojective function?

These kind of questions are very natural and are studied a lot in other areas of combinatorics (designs, codes, finite geometry, ...).

Planar functions and semifields

There are many biprojective planar functions.

Example (Göloglu, K., 2022)

Let $K = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, m even and set

$$F(x, y) = (x^{q+1} + by^{q+1}, x^r y + (a/b)xy^r),$$

where p odd, $q = p^k$ for some $1 \leq k \leq m-1$, $r = p^{k+m/2}$, $b \in \mathbb{F}_{p^m}$ is a non-square, $a \in \mathbb{F}^*_{p^{m/2}}$, $m/\gcd(k, m)$ is odd.

Planar functions are interesting in finite geometry because of their connection to commutative semifields.

Semifields

Definition

A (finite) semifield $\mathbb{S} = (S, +, \circ)$ is a finite set S equipped with two operations $(+, \circ)$ satisfying the following axioms.

(S1) $(S, +)$ is a group.

(S2) For all $x, y, z \in S$,

- $x \circ (y + z) = x \circ y + x \circ z$,
- $(x + y) \circ z = x \circ z + y \circ z$.

(S3) For all $x, y \in S$, $x \circ y = 0$ implies $x = 0$ or $y = 0$.

(S4) There exists an element $e \in \mathbb{S}$ such that $e \circ x = x \circ e = x$ for all $x \in \mathbb{S}$.

If (S4) does not hold we call the structure a presemifield.

Basic properties

Every presemifield can be turned into a semifield easily using *Kaplansky's trick.*

The additive group of a semifield $(\mathbb{S}, +, \circ)$ is always an elementary abelian p-group.

We can thus identify the additive group of a semifield $\mathbb{S}$ with the additive group of the finite field $\mathbb{F}_{p^n}$.

If $(\mathbb{S}, +, \circ)$ is a commutative semifield then $F(x) = x \circ x$ is a planar function.

If F is a quadratic planar function then $x \circ y = F(x + y) - F(x) - F(y)$ defines a commutative semifield.

Connections

Every semifield can be used to construct translation planes.

There is a 1-to-1 relation between semifields and rank-metric codes with certain optimal parameters.

How is equivalence of commutative semifields related to equivalence of planar functions?

Constructions of projective planes with finite fields

A projective plane is a set of lines and points such that

- There is exactly one line going through any 2 points.
- Two lines intersect in precisely one 1 point.
- There are four points such that no line is incident with more than 2 of them.

Constructions of projective planes with finite fields

Define the set of points as $\mathbb{F}_q \times \mathbb{F}_q$, (a) for any $a \in \mathbb{F}_q$, (∞) .

Define the set of lines via

$[m, k] = \{(m)\} \cup \{(x, y) \in \mathbb{F}_q^2 \colon mx + y = k\}$,

$[m] = \{(\infty)\} \cup \{(m, y) \in \mathbb{F}_q^2 \colon y \in \mathbb{F}_q\}$,

$[\infty] = \{(\infty)\} \cup \{(m) \colon m \in \mathbb{F}_q\}$.

Constructions of projective planes with finite fields

Define the set of points as $\mathbb{F}_q \times \mathbb{F}_q$, (a) for any $a \in \mathbb{F}_q$, (∞) .

Define the set of lines via

$[m,k] = \{(m)\} \cup \{(x,y) \in \mathbb{F}_q^2 \colon mx + y = k\}$,

$[m] = \{(\infty)\} \cup \{(m,y) \in \mathbb{F}_q^2 \colon y \in \mathbb{F}_q\}$,

$[\infty] = \{(\infty)\} \cup \{(m) \colon m \in \mathbb{F}_q\}$.

Important: $mx + y = k$ is uniquely solvable! Not important: associativity and commutativity of multiplication.

The same construction works with semifields!

Definition (Isotopy)

Two semifields $\mathbb{S}_1 = (\mathbb{F}_p^n, +, \circ_1)$ and $\mathbb{S}_2 = (\mathbb{F}_p^n, +, \circ_2)$ are *isotopic* if there exist $\mathbb{F}_p$-linear bijections L, M and N of $\mathbb{F}_{p^n}$ satisfying

$$N(x \circ_1 y) = L(x) \circ_2 M(y).$$

Such a triple $\gamma = (N, L, M)$ is called an *isotopism* between $\mathbb{S}_1$ and $\mathbb{S}_2$.

Definition (Autotopism and the Autotopism group)

The autotopism group $\mathrm{Aut}(\mathbb{S})$ of a semifield $\mathbb{S} = (\mathbb{F}_p^n, +, \circ)$ is defined by

$$\mathrm{Aut}(\mathbb{S}) = \{(N, L, M) \in \mathrm{GL}(\mathbb{F}_{p^n})^3 \colon N(x \circ y) = L(x) \circ M(y)\}.$$

Two semifields are isotopic iff the associated projective planes are isomorphic iff the associated rank-metric codes are isomorphic.

It turns out that isotopy of semifields is a slightly more general concept than equivalence of planar functions!

Theorem (Coulter, Henderson)

Two quadratic planar functions F, G are equivalent if and only if there exists an isotopism of the form (N, L, L) between their associated semifields.

It is thus better to work with the semifields when determining equivalence since the equivalence relation is more general.

"Biprojective" semifields

We are interested in special bivariate constructions where $K = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ and

$$(x, y) \circ (u, v) = (f(x, y, u, v), g(x, y, u, v)),$$

and f, g are homogeneous of degree $q + 1$ (resp. $r + 1$) where q, r are powers of p.

This is a generalization also to non-commutative semifields!

Example (Gölöglu, K., 2022)

Let $K = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, m even and set

$$(x, y) \circ (u, v) = (x^q u + x u^q + B(y^q v + y v^q), x^r v + y u^r + a/B(y v^r + y^r v)),$$

where p odd, $q = p^k$ for some $1 \leq k \leq m - 1$, $r = p^{k+m/2}$, $B \in \mathbb{F}_{p^m}$ is a non-square, $a \in \mathbb{F}^*_{p^{m/2}}$, $m/\gcd(k, m)$ is odd.

Recognizing the same nice structure

We are interested in special bivariate constructions where $K = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ and

$$(x, y) \circ (u, v) = (f(x, y, u, v), g(x, y, u, v)),$$

and f, g are homogeneous of degree $q + 1$ (resp. $r + 1$) where q, r are powers of p.

The same structure occurs in the autotopism group! Namely, if $L = M = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ then

$$L(x, y) \circ M(u, v) = (a^{q+1} f(x, y, u, v), a^{r+1} g(x, y, u, v)),$$

so (N, L, M) with $N = \begin{pmatrix} a^{q+1} & 0 \\ 0 & a^{r+1} \end{pmatrix}$ is an autotopism for any $a \in \mathbb{F}_{p^m}^{\times}$.

$\Longrightarrow$ These semifields always have a cyclic subgroup in their autotopism group of order $p^m - 1$.

The same technique we used for equivalence of the Boolean functions (Sylow groups etc.) works (with slight modifications) also for semifields!

We can thus directly work with semifields, even non-commutative ones where there is no connection to planar functions.

The results

We can use this approach to get precise conditions when two "biprojective" semifields are isotopic or not. This leads to

Theorem

The number of non-isotopic (commutative) semifields of size p^n in the Göloglu-K. family is around $p^{n/4}$.

The same result holds also for planar functions.

The previous best bound for commutative semifields of odd order was quadratic in n (Zhou-Pott semifields)!

This family is thus by far the biggest one (at least for now).

Counting...

The same approach applied to the biprojective (non-commutative) Taniguchi semifield construction:

Theorem

The number of non-isotopic semifields of size p^n in the Taniguchi family is around $p^{n/2+s}$ where s is the largest divisor of $n/2$ with $2s \neq n/2$.

This improves the lower bound for the number of odd order semifields (previous best was around $p^{n/2}$).

Where to go from here?

Soon: Similar results for the (non-commutative) Knuth semifields quadratic over a weak nucleus.
Bonus: Complete determination of the autotopism groups.

This corresponds to a determination of the collineation group of the associated projective planes and solves 60 year old conjectures by Hughes and Albert.

Constructions of rank-metric codes similar to "biprojective" semifields

Summary

Studying symmetries (automorphisms, autotopisms,...) is very useful for finding new extremal structures and classifying them up to equivalence!

Many techniques and properties can be applied and found in different combinatorial structures (Boolean functions, finite geometry, codes, designs, ...)

It helps to keep your eyes open!

The talk is based on three papers available on the arXiv:

Göloğlu, F., Kölsch, L.: Equivalences of biprojective almost perfect nonlinear functions.

Göloğlu, F., Kölsch, L.: An exponential bound on the number of non-isotopic commutative semifields. To appear in *Transactions of the American Mathematical Society*.

Göloğlu, F., Kölsch, L.: Counting the number of non-isotopic Taniguchi semifields.

Thank you for your attention!

The talk is based on three papers available on the arXiv:

Göloğlu, F., Kölsch, L.: Equivalences of biprojective almost perfect nonlinear functions.

Göloğlu, F., Kölsch, L.: An exponential bound on the number of non-isotopic commutative semifields. To appear in *Transactions of the American Mathematical Society*.

Göloğlu, F., Kölsch, L.: Counting the number of non-isotopic Taniguchi semifields.