Counting the number of non-isomorphic members in infinite families of combinatorial objects

Lukas Kölsch

University of South Florida

(partly based on joint work with Faruk Gologlu)

The setting

- When constructing infinite families of combinatorial objects (designs, difference sets, codes, graphs,...), we often want to count the (asymptotic) size of the family.
- I stumbled on this question via this family of *planar functions*

Example (Göloğlu, K., 2021)

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

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

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

The setting

Example (Göloğlu, K., 2021)

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

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

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

Definition (Planar function)

Let $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ be function. We call F planar, if $x \mapsto F(x+a) - F(x)$ is a bijection on $\mathbb{F}_p^n$ for all non-zero $a \in \mathbb{F}_p^n$.

Planar functions can be used to construct non-desarguesian projective planes, difference sets, semifields, rank-metric codes with optimal parameters etc.

The setting

Question

Which choices of a, b (and k) lead to different planar functions? In other words: How big is our family?

When do we consider planar functions as *different*?

Definition (Equivalence for planar functions)

Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ be a planar function. If $L_1, L_2 \in \mathrm{GL}(n, p)$ then $G = L_1 \circ F \circ L_2$ is also planar. We call F and G equivalent.

If we want to check if F, G are equivalent, we need to check if $L_1, L_2 \in \mathrm{GL}(n, p)$ exist s.t. $G = L_1 \circ F \circ L_2$.

The setting

Definition (Automorphism group for planar functions)

Let $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ be a planar function. We set

$$\mathrm{Aut}(F) = \{(L_1, L_2) \in \mathrm{GL}(n,p)^2 \colon F = L_1 \circ F \circ L_2\} \leq \mathrm{GL}(n,p) \times \mathrm{GL}(n,p).$$

Lemma

Let $F, G\colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ be equivalent planar functions. Then there exists $g \in \mathrm{GL}(n,p) \times \mathrm{GL}(n,p)$ s.t.

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

Equivalent functions have conjugate automorphism groups.

Lemma

Let $F, G \colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ *be equivalent planar functions. Then there exists* $g \in \mathrm{GL}(n,p) \times \mathrm{GL}(n,p)$ *s.t.*

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

This is very easy to see and generalizes to basically all notions of equivalence on combinatorial objects we know.

General setup for combinatorial objects:

- We have an equivalence relation on our combinatorial object.
- We define an automorphism group in a natural way that is embedded in an ambient group.
- The lemma above will hold (group action exercise for undergrads)

Object	Ambient group
Graphs	S_n
Designs	S_n
Linear Hamming codes	subgroup of $\Gamma L(n, q)$
Linear Rank-metric codes	$\Gamma L(n, q)$
Spreads	$\Gamma L(n, q) \times \Gamma L(n, q)$
$\vdots$	$\vdots$

Strategy

Lemma

Let F, G be equivalent combinatorial objects. Then there exists g in the ambient group s.t.

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

- Determining the entire Automorphism group is usually as hard as determining if two objects are isomorphic or not.
- If we can explicitly find easily recognizable subgroups of $\mathrm{Aut}(F)$, we can still use this lemma.
- Since we try to determine isomorphy of members of the same infinity family, we suspect that automorphism groups have similar structures (often even isomorphic).

Back to the starting example

Example (Göloğlu, K., 2021)

Let $F_{a,b,k} : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ defined via

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

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

We try to find some simple automorphisms, i.e. linear mappings L_1, L_2 s.t. $F_{a,b,k} = L_1 \circ F_{a,b,k} \circ L_2$.

Back to the starting example

Example (Göloğlu, K., 2021)

Let $F_{a,b,k} : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ defined via

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

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

We try to find some simple automorphisms, i.e. linear mappings L_1, L_2 s.t. $F_{a,b,k} = L_1 \circ F_{a,b,k} \circ L_2$.
Identify: $L_1 = \begin{pmatrix} 1/z^{q+1} & 0 \\ 0 & 1/z^{r+1} \end{pmatrix}$, $L_2 = \left(\begin{smallmatrix} z & 0 \\ 0 & z \end{smallmatrix}\right)$ for $z \in \mathbb{F}^*_{p^m}$.

Back to the starting example

Example (Göloğlu, K., 2021)

Let $F_{a,b,k} : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ defined via

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

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

We try to find some simple automorphisms, i.e. linear mappings L_1, L_2 s.t. $F_{a,b,k} = L_1 \circ F_{a,b,k} \circ L_2$.
Identify: $L_1 = \begin{pmatrix} 1/z^{q+1} & 0 \\ 0 & 1/z^{r+1} \end{pmatrix}$, $L_2 = \left(\begin{smallmatrix} z & 0 \\ 0 & z \end{smallmatrix}\right)$ for $z \in \mathbb{F}^*_{p^m}$.
So $\mathrm{Aut}(F_{a,b,k})$ contains a cyclic subgroup H of size $p^m - 1$, no matter the choice of a, b, k.

Back to the starting example

So $\mathrm{Aut}(F_{a,b,k})$ contains a cyclic subgroup H of size $p^m - 1$, no matter the choice of a, b, k.

Proof idea:

- Assume $F_{a,b,k}, F_{a',b',k'}$ are equivalent. Then $\mathrm{Aut}(F_{a,b,k})$ is conjugate to $\mathrm{Aut}(F_{a',b',k'})$.
- Show that then the cyclic subgroups we just identified have to be conjugate as well (use Sylow groups)
- Try to arrive at a contradiction (or find an equivalence).

In detail...

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

Show that two functions F_1, F_2 in the family 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 functions F_1, F_2 in the family 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 functions F_1, F_2 in the family 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 functions F_1, F_2 in the family 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 functions F_1, F_2 in the family 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 $\delta \in \mathrm{GL}(2m, p)^2$ 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 $\delta^{-1}S_1\delta = S_2$.

Last step:

Determine all $\delta \in \mathrm{GL}(n,p)^2$ such that $\delta^{-1} S_1 \delta = S_2$ and check if $\delta \in \mathrm{Aut}(F_2)$.

Recall $S_1 \leq H_1$, $S_2 \leq H_2$ and H_1, H_2 consist of mappings (L_1, L_2) where

$$L_2 = \left(\begin{smallmatrix} z & 0 \\ 0 & z \end{smallmatrix}\right) \text{ and } L_1 = \begin{pmatrix} 1/z^{q+1} & 0 \\ 0 & 1/z^{r+1} \end{pmatrix}.$$

Some calculations show that one can reduce everything to the case where the value of q, r for the two functions coincide, i.e. $S_1 = S_2$.

So: Everything is reduced to finding autotopisms δ that satisfy $\delta^{-1} S_1 \delta = S_1$, i.e. $\delta \in N_{\mathrm{GL}(2m,p)^2}(S_1)$.

A straight-forward calculation shows $N_{\mathrm{GL}(2m,p)^2}(S_1) = \Gamma L(2, p^m)^2$.

Reflections on the technique

This technique used the existence of a special subgroup in the automorphism group to prove that possible isomorphisms have to be contained in $\Gamma L(2, p^m)^2$.

It is thus much more general and can be applied to all functions of the form

$$F(x, y) = (f(x, y), g(x, y)),$$

where f, g are homogeneous polynomials.

Results

Example (Göloğlu, K., 2023)

Let $F_{a,b,k} : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ defined via

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

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

Theorem (Göloğlu, K., 2023)

Let $F_{k,a,b}$, $F_{k',a',b'}$ be planar functions from the family on $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

(i) *$F_{k,a,b}$ is equivalent to $F_{m-k,a',b}$ for $a' = b^{Q+1}/a$ and arbitrary q.*

(ii) *$F_{k,a,b}$ is equivalent to $F_{k,a',b'}$ for arbitrary q, b, b', a and a suitable choice for a'.*

(iii) *There are at most $2m$ different a' such that $F_{q,a,b}$ is equivalent to $F_{q,a'b}$.*

(iv) *No other equivalences exist.*

Theorem (Göloğlu, K., 2023)

The number of inequivalent members in the family on $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ is around $p^{m/2}$.

Theorem (Göloğlu, K., 2023)

The number of inequivalent members in the family is around $p^{m/2}$ on fields $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

The previous best bound for the number of inequivalent planar functions was quadratic in m (Zhou,Pott, 2011).

Other examples of this technique

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 $y = 0$.

Basic properties

If $\circ$ is associative then $\mathbb{S}$ is essentially a finite field (Wedderburn's Theorem).

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 vector space $\mathbb{F}_p^n$.

Semifields are in one to one correlation to translation planes whose duals are also translation planes, as well as certain maximum rank distance codes.

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 rank-metric codes are equivalent iff the corresponding planes are isomorphic.

A family of semifields by Taniguchi (2019)

The Taniguchi semifields are defined on $\mathbb{F}_p^n \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ with $n = 2m$ via the semifield multiplication

$$(x, y) * (u, v) = ((x^q u + \alpha x u^q)^{q^2} - a(x^q v - \alpha u^q y)^q - b(y^q v + \alpha y v^q), xv + yu),$$

where

- $q = p^k$ for some $1 \leq k \leq m - 1$,
- $-\alpha$ is not a $(q-1)$-st power, and
- the projective polynomial $P_{q,a,b}(x) = x^{q+1} + ax + b$ has no roots in $\mathbb{F}_{p^m}$.

Question

Which choices of α, a, b, k yield non-isotopic semifields?

$$(x,y)*(u,v) = ((x^q u + \alpha x u^q)^{q^2} - a(x^q v - \alpha u^q y)^q - b(y^q v + \alpha y v^q), xv + yu)$$

We try to apply out technique: Find autotopisms $N(x*y) = L(x)*M(y)$.

$$(x,y)*(u,v) = ((x^q u + \alpha x u^q)^{q^2} - a(x^q v - \alpha u^q y)^q - b(y^q v + \alpha y v^q), xv + yu)$$

We try to apply out technique: Find autotopisms $N(x*y) = L(x)*M(y)$. Equivalent to:

$$(x,y)\circ(u,v) = (x^q u + \alpha^{q^2} x u^q - a(x v^q - \alpha^q u y^q) - b(y^q v + \alpha y v^q), x v^{q^2} + y^{q^2} u).$$

$$N = \begin{pmatrix} z^{q+1} & 0 \\ 0 & z^{q^2+1} \end{pmatrix}, \quad L = M = \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}$$

yields an autotopism. So we have again a cyclic group of autotopisms of size $p^m - 1$.

Counting Taniguchi semifields

We have the exact same setup as before: A cyclic subgroup of the autotopism group of size $p^m - 1$.

Same techniques apply.
We achieve precise conditions on α, a, b, k when two Taniguchi semifields are isotopic.

Theorem (Göloğlu, K., 2024)

There are around p^{m+s} non-isotopic Taniguchi semifields of order p^{2m} where s is the largest divisor of m with $2s \neq m$.

Best currently known bound for the number of odd order semifields (translation planes whose duals are translation planes; full rank MRD codes).

Some more examples and notes

We also applied the techniques to APN functions and counted the number of inequivalent functions is several infinite families.

The technique is not new per se — several examples can be found in the literature, e.g. (Biliotti, Jha, Johnson, 1999), (Dempwolff, 2015), (Yoshiara, 2013), who used similar ideas for different combinatorial objects.

I did not invent this technique.

Some more examples and notes

We also applied the techniques to APN functions and counted the number of inequivalent functions is several infinite families.

The technique is not new per se — several examples can be found in the literature, e.g. (Biliotti, Jha, Johnson, 1999), (Dempwolff, 2015), (Yoshiara, 2013), who used similar ideas for different combinatorial objects.

I did not invent this technique.

Consider these ideas if you want to count the asymptotic size of an infinite family of objects.

Thank you for your attention!

The talk is based on three papers, all joint work with Faruk Göloğlu:

"An exponential bound on the number of non-isotopic commutative semifields." *Transactions of the American Mathematical Society* (2023)

"Counting the number of non-isotopic Taniguchi semifields." *Designs, Codes and Cryptography* (2024)

"Equivalences of biprojective almost perfect nonlinear functions." To appear in *Combinatorial Theory*.