Constructing designs using functions

Robert Coulter

Department of Mathematical Sciences
University of Delaware
coulter@udel.edu

This is joint work with Bradley Fain

February 2024

First Part

Definitions mostly

Some history too

An important class of polynomials

Definition

A polynomial $L \in \mathbb{F}_{p^e}[x]$ is called a *linearized polynomial* if

$$L(x) = \sum_i a_i x^{p^i}.$$

An important class of polynomials

Definition
A polynomial $L \in \mathbb{F}_{p^e}[x]$ is called a *linearized polynomial* if

$$L(x) = \sum_i a_i x^{p^i}.$$

Such polynomials represent all linear transformations of $\mathbb{F}_{p^e}$ when viewed as a vector space over $\mathbb{F}_p$. In particular, they satisfy

$$L(x+y) = L(x) + L(y) \text{ for all } x, y \in \mathbb{F}_{p^e}.$$

An important class of polynomials

Definition
A polynomial $L \in \mathbb{F}_{p^e}[x]$ is called a *linearized polynomial* if

$$L(x) = \sum_i a_i x^{p^i}.$$

Such polynomials represent all linear transformations of $\mathbb{F}_{p^e}$ when viewed as a vector space over $\mathbb{F}_p$. In particular, they satisfy

$$L(x + y) = L(x) + L(y) \text{ for all } x, y \in \mathbb{F}_{p^e}.$$

A linearized polynomial $L \in \mathbb{F}_q[x]$ induces a permutation under evaluaton (is a PP) over $\mathbb{F}_q$ if and only if the only root of $L(x)$ in $\mathbb{F}_q$ is 0.
(If you think about this in terms of a non-singular linear transformation, then we're talking about the size of the null space.)

An important class of polynomials

Definition

A polynomial $L \in \mathbb{F}_{p^e}[x]$ is called a *linearized polynomial* if

$$L(x) = \sum_i a_i x^{p^i}.$$

Such polynomials represent all linear transformations of $\mathbb{F}_{p^e}$ when viewed as a vector space over $\mathbb{F}_p$. In particular, they satisfy

$$L(x+y) = L(x) + L(y) \text{ for all } x, y \in \mathbb{F}_{p^e}.$$

A linearized polynomial $L \in \mathbb{F}_q[x]$ induces a permutation under evaluaton (is a PP) over $\mathbb{F}_q$ if and only if the only root of $L(x)$ in $\mathbb{F}_q$ is 0.
(If you think about this in terms of a non-singular linear transformation, then we're talking about the size of the null space.)
And linearized polynomials are closed under reduction modulo $x^q - x$.

Another important class of polynomials

Definition

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

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

Another important class of polynomials

Definition

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

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

They are mostly significant because they are precisely the polynomials whose non-trivial differential operators $D(x + a) - D(x) - D(a)$ are all linearized polynomials.

Another important class of polynomials

Definition

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

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

They are mostly significant because they are precisely the polynomials whose non-trivial differential operators $D(x+a) - D(x) - D(a)$ are all linearized polynomials.

And DO polynomials are closed under reduction modulo $x^q - x$.

The interplay between DOs and linearized polynomials

So DO polynomials are precisely those polynomials whose non-trivial differential operators $D(x+a) - D(x) - D(a)$ are all linearized polynomials However, this is not their only important connection.

$$L(x) = \sum_i a_i x^{p^i}$$
$$D(x) = \sum_{i,j} a_{ij} x^{p^i + p^j}$$

Think about what happens with composition…

The interplay between DOs and linearized polynomials

So DO polynomials are precisely those polynomials whose non-trivial differential operators $D(x+a) - D(x) - D(a)$ are all linearized polynomials However, this is not their only important connection.

$$L(x) = \sum_i a_i x^{p^i}$$
$$D(x) = \sum_{i,j} a_{ij} x^{p^i + p^j}$$

Think about what happens with composition...
Yep, $L(D)$ and $D(L)$ are both DOs, even after reduction.
This can lead to the study of DO polynomials under the action of the general linear group, say, since the general linear group is nothing more than the group of all non-singular transformations – i.e. the group of linearized PPs working modulo $x^q - x$.

Incidence structures I

Definition

A connected incidence structure $\mathcal{P}$ is a *projective plane* if

- Every two points lie on a unique line.
- Every two lines intersect at a unique point.
- There are at least 4 points, no three of which are collinear.

These axioms force $\mathcal{P}$ to have the following properties:

- the number of points on each line is the same as the number of lines through each point.
- the same number of points as lines.

Incidence structures I

Definition

A connected incidence structure $\mathcal{P}$ is a *projective plane* if

- $\oplus$ Every two points lie on a unique line.
- $\oplus$ Every two lines intersect at a unique point.
- $\oplus$ There are at least 4 points, no three of which are collinear.

These axioms force $\mathcal{P}$ to have the following properties:

- $\oplus$ the number of points on each line is the same as the number of lines through each point. $n+1$
- $\oplus$ the same number of points as lines. n^2+n+1

We call this important invariant n the *order* of $\mathcal{P}$.

Affine and projective planes

If you have a projective plane and you delete any one line and all of the points on it, then you obtain what is known as an *affine plane*.

The affine plane satisfies almost all of the axioms of a projective plane (there's a slight fudge in the 2 lines intersecting at a unique point part).

Affine planes are equivalent to projective planes for if you have an affine plane, then it can only be completed in a single way to obtain a projective plane.

This concept of "completing" or "extending" is a central technique in projective geometry.

The big open problems

There are two major open problems in the area.

The big open problems

There are two major open problems in the area.

- $\oplus$ It is conjectured that any plane of prime order is classical – i.e. you can construct it by defining vertical lines and slope lines $y = mx + c$ over $\mathbb{F}_p$.

The big open problems

There are two major open problems in the area.

- It is conjectured that any plane of prime order is classical – i.e. you can construct it by defining vertical lines and slope lines $y = mx + c$ over $\mathbb{F}_p$.
  Most geometers believe this is true.

The big open problems

There are two major open problems in the area.

- $\oplus$ It is conjectured that any plane of prime order is classical – i.e. you can construct it by defining vertical lines and slope lines $y = mx + c$ over $\mathbb{F}_p$.
  Most geometers believe this is true.
- $\oplus$ It is conjectured that all planes must have prime power order.

The big open problems

There are two major open problems in the area.

- $\oplus$ It is conjectured that any plane of prime order is classical – i.e. you can construct it by defining vertical lines and slope lines $y = mx + c$ over $\mathbb{F}_p$.
  Most geometers believe this is true.
- $\oplus$ It is conjectured that all planes must have prime power order.
  There is no consensus among geometers.

Incidence structures II

Definition

A connected incidence structure $\mathcal{S}$ is a *semibiplane* if

- $\oplus$ Every two points lie on 0 or 2 lines.
- $\oplus$ Every two lines intersect at 0 or 2 points.

Definition

A connected incidence structure $\mathcal{S}$ is a *biplane* if

- $\oplus$ Every two points lie on 2 lines.
- $\oplus$ Every two lines intersect at 2 points.

For biplanes we have the same number of points on a line and lines through a point: $n + 2$.
And the number of points and lines in the entire structure are the same: $1 + (n + 2)(n + 1)/2$.
Again we call n the order.

The big open problems

The biggest problem here concerns biplanes.

We only know of 18 examples, the largest ones having order 11.

The big open problems

The biggest problem here concerns biplanes.

We only know of 18 examples, the largest ones having order 11.

And we have literally no idea what's going on.

The big open problems

The biggest problem here concerns biplanes.

We only know of 18 examples, the largest ones having order 11.

And we have literally no idea what's going on.

The biggest problem concerning semibiplanes is probably:

There is a method for constructing projective planes from specific types of semibiplanes, and when it works it produces "exotic" examples.

But so far it's only produced 2 new examples because we only have 2 examples of semibiplanes that satisfy the criteria!

The big open problems

The biggest problem here concerns biplanes.

We only know of 18 examples, the largest ones having order 11.

And we have literally no idea what's going on.

The biggest problem concerning semibiplanes is probably:

There is a method for constructing projective planes from specific types of semibiplanes, and when it works it produces "exotic" examples.

But so far it's only produced 2 new examples because we only have 2 examples of semibiplanes that satisfy the criteria!

This is not like the biplane problem – we have infinitely many examples of semibiplanes, its just that the criteria needed seems to be very rare.

Incidence structures III

Definition

A connected incidence structure $\mathcal{S}$ is a *semisymmetric design (SSD)* if there exists some integer $\lambda > 0$ such that

- $\oplus$ Every two points lies on 0 or λ lines.
- $\oplus$ Every two lines intersect at 0 or λ points.

Here λ is often called the *incidence parameter*.

If $\lambda = 1$, the SSD is more commonly called a partial plane.

If $\lambda = 2$, the SSD is just a semibiplane.

Some facts about SSDs

Theorem [Wild, 1981]
Let S be a semisymmetric design with incidence parameter $\lambda > 1$. Then S has the following properties,

(i) there is a positive integer k such that every point is on k lines and every line contains k points,

(ii) the number of points is equal to the number of lines, usually denoted by v,

(iii) every point has $k(k-1)/\lambda$ neighbours,

(iv) $v \geq k(k-1)/\lambda + 1$,

(v) $2\lambda \mid vk(k-1)$.

Because of these results we usually write $\mathrm{SSD}(v, k, \lambda)$ for the SSD.

The big open problems

If we generalise the biplane definition to $\lambda > 2$, we know even less than we do for biplanes.

The big open problems

If we generalise the biplane definition to $\lambda > 2$, we know even less than we do for biplanes.

And we have even less idea what's going on.

The big open problems

If we generalise the biplane definition to $\lambda > 2$, we know even less than we do for biplanes.

And we have even less idea what's going on.

At present, there is also no theory on how to complete partial planes or semibiplanes or SSDs to their regular counterparts.

There is some partial success for partial planes, but we have no idea for any $\lambda \geq 2$.

It was hoped that this approach might lead to breaking open the general problem, but nowawdays at least some combinatorists seem to think it is a dead-end.

Second Part

Definitions of the functions

Sort of a history

A long long time ago. . .

A long long time ago...

Definition (Dembowski & Ostrom, 1968)
Let $\mathcal{G}, \mathcal{H}$ be finite abelian groups, written additively.
Let $f : \mathcal{G} \to \mathcal{H}$.
We say f is

planar

if, for every $a \in \mathcal{G}, b \in \mathcal{H}$ with $a \neq 0$, the equation

$$f(x+a) - f(x) = b$$

has a unique solution $x \in \mathcal{G}$.

Definition (Nyberg, 1993)
Let $\mathcal{G}, \mathcal{H}$ be finite abelian groups, written additively.
Let $f : \mathcal{G} \to \mathcal{H}$.
We say f is

almost perfect non-linear (APN)

if, for every $a \in \mathcal{G}, b \in \mathcal{H}$ with $a \neq 0$, the equation

$$f(x+a) - f(x) = b$$

has at most 2 solutions $x \in \mathcal{G}$.

A not-as-long as a not-as-long time ago...

Definition (Coulter & Henderson, 1999)
Let $\mathcal{G}, \mathcal{H}$ be finite abelian groups, written additively.
Let $f : \mathcal{G} \to \mathcal{H}$.
We say f is

semiplanar

if, for every $a \in \mathcal{G}, b \in \mathcal{H}$ with $a \neq 0$, the equation

$$f(x + a) - f(x) = b$$

has either 0 or 2 solutions $x \in \mathcal{G}$.

APN vs semiplanar

Why the two definitions?

Revisiting the proof of the following result is maybe instructive:

Lemma

If $f : \mathcal{G} \to \mathcal{H}$ is planar, then $\#\mathcal{G}$ must be odd.

APN vs semiplanar

Why the two definitions?

Revisiting the proof of the following result is maybe instructive:

Lemma

If $f : \mathcal{G} \to \mathcal{H}$ is planar, then $\#\mathcal{G}$ must be odd.

Suppose f is planar and $\#\mathcal{G}$ is even.

Then there exists an involution $t \in \mathcal{G}$ (an element of order 2).

As f is planar, the map $x \mapsto f(x+t) - f(x)$ is a bijection.

That means there exists a unique solution x_0 to

$$f(x_0 + t) - f(x_0) = 0.$$

APN vs semiplanar

Why the two definitions?
Revisiting the proof of the following result is maybe instructive:

Lemma
If $f : \mathcal{G} \to \mathcal{H}$ is planar, then $\#\mathcal{G}$ must be odd.

Suppose f is planar and $\#\mathcal{G}$ is even.
Then there exists an involution $t \in \mathcal{G}$ (an element of order 2).
As f is planar, the map $x \mapsto f(x+t) - f(x)$ is a bijection.
That means there exists a unique solution x_0 to

$$f(x_0 + t) = f(x_0).$$

APN vs semiplanar

Why the two definitions?
Revisiting the proof of the following result is maybe instructive:

Lemma
If $f : \mathcal{G} \to \mathcal{H}$ is planar, then $\#\mathcal{G}$ must be odd.

Suppose f is planar and $\#\mathcal{G}$ is even.
Then there exists an involution $t \in \mathcal{G}$ (an element of order 2).
As f is planar, the map $x \mapsto f(x+t) - f(x)$ is a bijection.
That means there exists a unique solution x_0 to

$$f(x_0 + t) = f(x_0).$$

But then $f((x_0+t)+t) - f(x_0+t) = f(x_0) - f(x_0+t) = 0$, so that $x_0 + t$ is also a solution, a contradiction.

APN vs semiplanar

Why the two definitions?
Revisiting the proof of the following result is maybe instructive:

Lemma
If $f : \mathcal{G} \to \mathcal{H}$ is planar, then $\#\mathcal{G}$ must be odd.

Suppose f is planar and $\#\mathcal{G}$ is even.
Then there exists an involution $t \in \mathcal{G}$ (an element of order 2).
As f is planar, the map $x \mapsto f(x+t) - f(x)$ is a bijection.
That means there exists a unique solution x_0 to

$$f(x_0 + t) = f(x_0).$$

But then $f((x_0+t)+t) - f(x_0+t) = f(x_0) - f(x_0+t) = 0$, so that $x_0 + t$ is also a solution, a contradiction.

So whenever we look at the derivative in the direction of an involution, solutions will come in pairs.

APN vs semiplanar

So whenever we look at the derivative in the direction of an involution, solutions will come in pairs.

APN vs semiplanar

So whenever we look at the derivative in the direction of an involution, solutions will come in pairs.

Now consider the two definitions over a finite field of characteristic 2.

APN vs semiplanar

So whenever we look at the derivative in the direction of an involution, solutions will come in pairs.

Now consider the two definitions over a finite field of characteristic 2. In $\mathbb{F}_{2^e}$, the additive group (the relevant group to the definition) is an elementary abelian 2-group.

APN vs semiplanar

> *So whenever we look at the derivative in the direction of an involution, solutions will come in pairs.*

Now consider the two definitions over a finite field of characteristic 2. In $\mathbb{F}_{2^e}$, the additive group (the relevant group to the definition) is an elementary abelian 2-group.

That means every non-zero element is an involution.

So every derivative will have solutions coming in pairs and consequently APN and semiplanar coincide over finite fields of characteristic 2.

Over other groups, they mean different things.

Ago...

Definition (Coulter & Fain, 1999/2021)
Let $\mathcal{G}, \mathcal{H}$ be finite abelian groups, written additively.
Let $f : \mathcal{G} \to \mathcal{H}$ and $\lambda \geq 2$ be an integer.
We say f is

semiplanar of index λ

if, for every $a \in \mathcal{G}, b \in \mathcal{H}$ with $a \neq 0$, the equation

$$f(x + a) - f(x) = b$$

has either 0 or λ solutions $x \in \mathcal{G}$.

Third Part

Incidence structures from functions

Justifying why those functions just defined were just defined

The problem of connectivity (or connectedness, if you prefer)

An incidence structure for functions (planar version)

For $f : \mathcal{G} \to \mathcal{H}$, we define an incidence structure $I(\mathcal{G}, \mathcal{H}; f)$ as follows:

- $\oplus$ "Points" are the elements of $\mathcal{G} \times \mathcal{H}$,
- $\oplus$ "Lines" are the symbols $\mathcal{L}(a, b)$, $\mathcal{L}(c)$ where $a, c \in \mathcal{G}$ and $b \in \mathcal{H}$, and are defined by
- $\oplus$ $\mathcal{L}(a, b) = \{(x, f(x - a) + b) \ : \ x \in \mathcal{G}\}$, and
- $\oplus$ $\mathcal{L}(c) = \{(c, y) : y \in \mathcal{H}\}$

An incidence structure for functions (planar version)

For $f : \mathcal{G} \to \mathcal{H}$, we define an incidence structure $I(\mathcal{G}, \mathcal{H}; f)$ as follows:

- "Points" are the elements of $\mathcal{G} \times \mathcal{H}$,
- "Lines" are the symbols $\mathcal{L}(a, b)$, $\mathcal{L}(c)$ where $a, c \in \mathcal{G}$ and $b \in \mathcal{H}$, and are defined by
- $\mathcal{L}(a, b) = \{(x, f(x - a) + b) \ : \ x \in \mathcal{G}\}$, and
- $\mathcal{L}(c) = \{(c, y) : y \in \mathcal{H}\}$

One can think of these lines as lines of slope a and vertical lines.

Note how the whole structure $I(\mathcal{G}, \mathcal{H}; f)$ is dependent on f as the slope lines are dependent on f.

Intersection points

$$\mathcal{L}(a,b) = \{(x, f(x-a)+b) \ : \ x \in \mathcal{G}\}$$
$$\mathcal{L}(c) = \{(c,y) \ : \ y \in \mathcal{H}\}$$

Intersection points

$$\mathcal{L}(a,b) = \{(x, f(x-a)+b) \ : \ x \in \mathcal{G}\}$$
$$\mathcal{L}(c) = \{(c,y) \ : \ y \in \mathcal{H}\}$$

Consider the intersection points for the lines in $I(\mathcal{G},\mathcal{H};f)$. We have

$$\begin{aligned}
&\mathcal{L}(c) \cap \mathcal{L}(d) = \varnothing \\
&\mathcal{L}(c) \cap \mathcal{L}(a,b) = \{(c, f(c-a)+b)\}.
\end{aligned}$$

So zero or 1 intersection points involving vertical lines. And

Intersection points

$$\mathcal{L}(a,b) = \{(x, f(x-a)+b) \ : \ x \in \mathcal{G}\}$$
$$\mathcal{L}(c) = \{(c,y) \ : \ y \in \mathcal{H}\}$$

Consider the intersection points for the lines in $I(\mathcal{G},\mathcal{H};f)$. We have

$$\begin{aligned} &\mathcal{L}(c) \cap \mathcal{L}(d) = \varnothing \\ &\mathcal{L}(c) \cap \mathcal{L}(a,b) = \{(c, f(c-a)+b)\}. \end{aligned}$$

So zero or 1 intersection points involving vertical lines. And

$$\begin{aligned} \mathcal{L}(a,b) \cap \mathcal{L}(c,d) &= \{(x, f(x-a)+b) \ : \ f(x-a)+b = f(x-c)+d\} \\ &= \{(x, f(x-a)+b) \ : \ f(x-a) - f(x-c) = d-b\}. \end{aligned}$$

So when $a = c$, $\mathcal{L}(a,b) \cap \mathcal{L}(a,d) = \varnothing$ unless $b = d$.

For $a \neq c$, intersection points are tied to the derivatives of f.

Properties of the structure $I(\mathcal{G}, \mathcal{H}; f)$

Theorem (Dembowski & Ostrom, 1968)
Let $\mathcal{G}$ and $\mathcal{H}$ be finite abelian groups written additively where $\#\mathcal{G} = \#\mathcal{H} = n$. If $f : \mathcal{G} \to \mathcal{H}$ is a planar function, then $I(\mathcal{G}, \mathcal{H}; f)$ has the following properties.

(i) It has n^2 points and $n^2 + n$ lines.

(ii) Each line contains n points and each point is on $n + 1$ lines.

(iii) Every pair of points occur on a unique line. Every pair of lines intersect in 0 or 1 points.

(iv) For every point there are exactly $n^2 - 1$ other points defined by the lines through it; for every line there are exactly n^2 other lines intersecting it.

Projective planes from planar functions

Theorem (Dembowski & Ostrom, 1968)
A connected $I(\mathcal{G}, \mathcal{H}; f)$ is an affine plane if and only if $f : \mathcal{G} \to \mathcal{H}$ is a planar function.

Projective planes from planar functions

Theorem (Dembowski & Ostrom, 1968)
A connected $I(\mathcal{G}, \mathcal{H}; f)$ is an affine plane if and only if $f : \mathcal{G} \to \mathcal{H}$ is a planar function.

The only issue to be considered is whether or not the structure is connected.

However, since every point has $n^2 - 1$ neighbours, we see every point is connected to every other point.

Thus, planar functions *always* produce affine planes.

An incidence structure for functions (semiplanar version)

For $f : \mathcal{G} \to \mathcal{H}$, define $S(\mathcal{G}, \mathcal{H}; f)$ as follows:

- "Points" are the elements of $\mathcal{G} \times \mathcal{H}$,
- "Lines" are the symbols $\mathcal{L}(a, b)$ where $a \in \mathcal{G}$ and $b \in \mathcal{H}$, and are defined by
- $\mathcal{L}(a, b) = \{(x, f(x - a) + b) \ : \ x \in \mathcal{G}\}$.

An incidence structure for functions (semiplanar version)

For $f : \mathcal{G} \to \mathcal{H}$, define $S(\mathcal{G}, \mathcal{H}; f)$ as follows:

- $\oplus$ "Points" are the elements of $\mathcal{G} \times \mathcal{H}$,
- $\oplus$ "Lines" are the symbols $\mathcal{L}(a, b)$ where $a \in \mathcal{G}$ and $b \in \mathcal{H}$, and are defined by
- $\oplus$ $\mathcal{L}(a, b) = \{(x, f(x - a) + b) \ : \ x \in \mathcal{G}\}$.

What changed?

An incidence structure for functions (semiplanar version)

For $f : \mathcal{G} \to \mathcal{H}$, define $S(\mathcal{G}, \mathcal{H}; f)$ as follows:

- "Points" are the elements of $\mathcal{G} \times \mathcal{H}$,
- "Lines" are the symbols $\mathcal{L}(a, b)$ where $a \in \mathcal{G}$ and $b \in \mathcal{H}$, and are defined by
- $\mathcal{L}(a, b) = \{(x, f(x - a) + b) \ : \ x \in \mathcal{G}\}$.

What changed? Yes, we deleted the vertical lines.

An incidence structure for functions (semiplanar version)

For $f : \mathcal{G} \to \mathcal{H}$, define $S(\mathcal{G}, \mathcal{H}; f)$ as follows:

- "Points" are the elements of $\mathcal{G} \times \mathcal{H}$,
- "Lines" are the symbols $\mathcal{L}(a, b)$ where $a \in \mathcal{G}$ and $b \in \mathcal{H}$, and are defined by
- $\mathcal{L}(a, b) = \{(x, f(x - a) + b) \ : \ x \in \mathcal{G}\}$.

What changed? Yes, we deleted the vertical lines.

But why?!

How come you can just delete stuff?!

How come you can just delete stuff?!

A little known fact about projective planes is that the step from projective to affine through deleting a line is not the only reversible step one can do.

How come you can just delete stuff?!

A little known fact about projective planes is that the step from projective to affine through deleting a line is not the only reversible step one can do.

$$\begin{gathered}\text{Projective plane}\\ \Updownarrow\\ \textit{Delete any one line and all the points on it}\\ \Updownarrow\\ \text{Affine plane}\end{gathered}$$

How come you can just delete stuff?!

A little known fact about projective planes is that the step from projective to affine through deleting a line is not the only reversible step one can do.

Projective plane

$\Updownarrow$

Delete any one line and all the points on it

$\Updownarrow$

Affine plane

$\Updownarrow$

Delete all the lines of a single parallel class (the "vertical lines")

$\Updownarrow$

The defining component of the projective plane (just the "slope lines")

The structure $S(\mathcal{G}, \mathcal{H}; f)$

We're keeping the slope lines but throwing out the vertical lines.

Implications?

The structure $S(\mathcal{G}, \mathcal{H}; f)$

We're keeping the slope lines but throwing out the vertical lines.

Implications?

The structure remains dependent on the function f.

The structure $S(\mathcal{G}, \mathcal{H}; f)$

We're keeping the slope lines but throwing out the vertical lines.

Implications?

The structure remains dependent on the function f.

And the intersection points of slope lines are dependent on the derivatives, which means the derivatives of the function remain integral to understanding the incidence structure.

Properties of the structure $S(\mathcal{G}, \mathcal{H}; f)$

Theorem (Coulter & Henderson, 1999; Coulter & Fain, 2021)
Let $\mathcal{G}$ and $\mathcal{H}$ be finite abelian groups written additively where $\#\mathcal{G} = n$ and $\#\mathcal{H} = m$. If $f : \mathcal{G} \to \mathcal{H}$ is a semiplanar function of index $\lambda \geq 2$, then $S(\mathcal{G}, \mathcal{H}; f)$ has the following properties.

(i) It has nm points and nm lines.

(ii) Each line contains n points and each point is on n lines.

(iii) Every pair of points occur on 0 or λ lines and every pair of lines intersect in 0 or λ points.

(iv) For every point there are exactly $n(n-1)/\lambda$ other points defined by the lines through it.

SDDs from semiplanar functions

Theorem (Coulter & Henderson, 1999; Coulter & Fain, 2021)
Let $\#\mathcal{G} = n$ and $\#\mathcal{H} = m$.
A connected $S(\mathcal{G}, \mathcal{H}; f)$ is a SSD(nm, n, λ) if and only if $f : \mathcal{G} \to \mathcal{H}$ is a semiplanar function of index λ.

SDDs from semiplanar functions

Theorem (Coulter & Henderson, 1999; Coulter & Fain, 2021)
Let $\#\mathcal{G} = n$ and $\#\mathcal{H} = m$.
A connected $S(\mathcal{G}, \mathcal{H}; f)$ is a SSD(nm, n, λ) if and only if $f : \mathcal{G} \to \mathcal{H}$ is a semiplanar function of index λ.

Yes, there is that issue with connectivity...

Unlike the planar function situation, now we're only guaranteed that a point has (at best) roughly half the points in the structure as neighbours, so it's not quite as straightforward.

Is this structure connected or not?!

Theorem (Coulter & Henderson, 1999, 2004)
Let $f : \mathcal{G} \to \mathcal{H}$ be a semiplanar function of index 2. If the structure is not connected, then it splits into exactly two isomorphic semibiplanes.

This actually happens when $\#\mathcal{G} = \#\mathcal{H} = 4$.

Is this structure connected or not?!

Theorem (Coulter & Henderson, 1999, 2004)
Let $f : \mathcal{G} \to \mathcal{H}$ be a semiplanar function of index 2. If the structure is not connected, then it splits into exactly two isomorphic semibiplanes.

This actually happens when $\#\mathcal{G} = \#\mathcal{H} = 4$.

Theorem (Coulter & Henderson, 1999)
If $f : \mathcal{G} \to \mathcal{H}$ is a bijective semiplanar function of index 2 and $\#\mathcal{G} > 4$, then $S(\mathcal{G}, \mathcal{H}; f)$ is connected.

Is this structure connected or not?!

Theorem (Coulter & Henderson, 1999, 2004)
Let $f : \mathcal{G} \to \mathcal{H}$ be a semiplanar function of index 2. If the structure is not connected, then it splits into exactly two isomorphic semibiplanes.

This actually happens when $\#\mathcal{G} = \#\mathcal{H} = 4$.

Theorem (Coulter & Henderson, 1999)
If $f : \mathcal{G} \to \mathcal{H}$ is a bijective semiplanar function of index 2 and $\#\mathcal{G} > 4$, then $S(\mathcal{G}, \mathcal{H}; f)$ is connected.

Theorem (Yoshiara, 2010)
If $f : \mathcal{G} \to \mathcal{H}$ is a semiplanar function of index 2 and $\#\mathcal{G} > 4$, then $S(\mathcal{G}, \mathcal{H}; f)$ is connected.

Connectivity of $S(\mathcal{G}, \mathcal{H}; f)$ for semiplanar f

For $S \subseteq \mathcal{G}$, we use Span(S) to denote the subgroup of $\mathcal{G}$ that is generated by S – i.e. the closure of S.

Theorem (Coulter & Fain, 2021)
Let $f : \mathcal{G} \to \mathcal{H}$ be a semiplanar function of index $\lambda \geq 2$ and suppose wlog $f(0) = 0$. Define the set Γ_f by

$$\Gamma_f = \{(x, f(x)) : x \in \mathcal{G}\}.$$

Then $S(\mathcal{G}, \mathcal{H}; f)$ is connected if and only if $\mathrm{Span}(\Gamma_f) = \mathcal{G} \times \mathcal{H}$.

Connectivity of $S(\mathcal{G}, \mathcal{H}; f)$ for semiplanar f

Corollary

If $S(\mathcal{G}, \mathcal{H}; f)$ is connected, then $\mathrm{Span}(\mathrm{Im}(f)) = \mathcal{H}$.

Connectivity of $S(\mathcal{G}, \mathcal{H}; f)$ for semiplanar f

Corollary
If $S(\mathcal{G}, \mathcal{H}; f)$ is connected, then $\mathrm{Span}(\mathrm{Im}(f)) = \mathcal{H}$.

We thought this was a sufficient condition,

Connectivity of $S(\mathcal{G}, \mathcal{H}; f)$ for semiplanar f

Corollary

If $S(\mathcal{G}, \mathcal{H}; f)$ is connected, then $\mathrm{Span}(\mathrm{Im}(f)) = \mathcal{H}$.

We thought this was a sufficient condition, but there are some easy counterexamples.

The polynomial $f(x) = \mathrm{Tr}(x^2)$ over $\mathbb{F}_{q^2}$, with Tr the trace from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$, is semiplanar of index q (for $q \geq 5$). But it's easy to show...

- $S(\mathbb{F}_{q^2}, \mathbb{F}_{q^2}; f)$ and $S(\mathbb{F}_{q^2}, \mathbb{F}_{q^2}; f + x)$ are isomorphic, and
- $\mathrm{Span}(\mathrm{Im}(f)) = \mathbb{F}_q$ and $\mathrm{Span}(\mathrm{Im}(f + x)) = \mathbb{F}_{q^2}$.

The best we can do with connectivity

Theorem (Coulter & Fain, 2021)
Let $\mathcal{G}, \mathcal{H}$ be finite abelian groups of order n and m, respectively.
Let $f : \mathcal{G} \to \mathcal{H}$ be semiplanar of index $\lambda > 2$.
Then $S(\mathcal{G}, \mathcal{H}; f)$ is a collection of at most $\frac{m}{n}\lambda$ isomorphic SSDs.

The best we can do with connectivity

Theorem (Coulter & Fain, 2021)
Let $\mathcal{G}, \mathcal{H}$ be finite abelian groups of order n and m, respectively.
Let $f : \mathcal{G} \to \mathcal{H}$ be semiplanar of index $\lambda > 2$.
Then $S(\mathcal{G}, \mathcal{H}; f)$ is a collection of at most $\frac{m}{n}\lambda$ isomorphic SSDs.

Disappointingly, this is, in fact, the best we can do!

The function $f(x) = \mathrm{Tr}(x^2)$ where Tr is the trace from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is a semiplanar function of index q^{n-1}.

And we can prove that $S(\mathbb{F}_{q^n}, \mathbb{F}_{q^n}; f)$ is a collection of q^{n-1} isomorphic copies of a $\mathrm{SSD}(q^{n+1}, q^n, q^{n-1})$.

Fourth Part

Restrictions

Existence

Composition

Requirements for planar functions to exist

Requirements for planar functions to exist

There are some limitations on the groups involved:

- $\oplus$ $\#\mathcal{G} = \#\mathcal{H}$
- $\oplus$ $\mathcal{G}$ cannot contain an involution. So $\#\mathcal{G}$ must be odd.

Requirements for planar functions to exist

There are some limitations on the groups involved:

- $\oplus$ $\#\mathcal{G} = \#\mathcal{H}$
- $\oplus$ $\mathcal{G}$ cannot contain an involution. So $\#\mathcal{G}$ must be odd.

A further possible requirement is that both groups need to be elementary abelian p-groups.

J.C.D.S. Yaqub may have had a proof of this ("about 3 pages of hand-written notes"), but she died before sharing it with me.

Nowadays this is called Yaqub's conjecture, and if it's true, then the study of planar functions can be restricted to just the finite field case.

Requirements for semiplanar functions to exist ($\lambda \geq 2$)

There are only 2 conditions, and both are kind of trivial:

- $\oplus$ $\#\mathcal{G}/\#\mathcal{H} \leq \lambda$.
- $\oplus$ λ must divide $\#\mathcal{G}$.

Requirements for semiplanar functions to exist ($\lambda \geq 2$)

There are only 2 conditions, and both are kind of trivial:

- $\#\mathcal{G}/\#\mathcal{H} \leq \lambda$.
- λ must divide $\#\mathcal{G}$.

There was a combinatorial design conjecture akin to Yaqub's conjecture related to certain designs, but this was proven false by Mubayi via a construction over non-abelian groups.

His constructions, however, do not ever produce SSDs so his results do not preclude the possibilty that we can only construct these functions over elementary p-groups again.

Actual planar functions

Theorem (Coulter & Matthews, 1997)
Let $f(x) = x^{p^k+1} \in \mathbb{F}_{p^e}[x]$ with p odd.
Then f is planar if and only if $\frac{e}{\gcd(k,e)}$ is odd.

Yes, DO monomial examples.

Actual semiplanar functions (APN functions)

Since APN and semiplanar functions are one and the same over $\mathbb{F}_{2^e}$, we can cheat and just use APN examples here...

Theorem (Gold, 1968)
Let $f(x) = x^{2^k+1} \in \mathbb{F}_{2^e}[x]$.
Then f is APN/semiplanar of index 2 if and only if $\gcd(k, e) = 1$.

Actual semiplanar functions (APN functions)

Since APN and semiplanar functions are one and the same over $\mathbb{F}_{2^e}$, we can cheat and just use APN examples here...

Theorem (Gold, 1968)
Let $f(x) = x^{2^k+1} \in \mathbb{F}_{2^e}[x]$.
Then f is APN/semiplanar of index 2 if and only if $\gcd(k, e) = 1$.

Most in the room will be able to list at least several more examples, but I'm just going to leave it simple with this one...there's a reason, of course!

Actual semiplanar functions of index $\lambda > 2$

Theorem (Coulter & Fain, 2021)
Let $f(x) = x^{p^k+1} \in \mathbb{F}_{p^e}[x]$.
For $p = 2$, f is semiplanar of index $2^{\gcd(k,e)}$.
For p odd, we have the following:

(i) If $\frac{e}{\gcd(k,e)}$ is odd, then f is planar.

(ii) If $\frac{e}{\gcd(k,e)}$ is even, then f is semiplanar of index $p^{\gcd(k,e)}$.

Actual semiplanar functions of index $\lambda > 2$

Theorem (Coulter & Fain, 2021)
Let $f(x) = x^{p^k+1} \in \mathbb{F}_{p^e}[x]$.
For $p = 2$, f is semiplanar of index $2^{\gcd(k,e)}$.
For p odd, we have the following:

(i) If $\frac{e}{\gcd(k,e)}$ is odd, then f is planar.

(ii) If $\frac{e}{\gcd(k,e)}$ is even, then f is semiplanar of index $p^{\gcd(k,e)}$.

To be honest, this is kind of forced. The reason is pretty simple.

And if you've ever wondered why there is a prevalence of DOs among planar functions and APN functions, it is the same reason.

Why DO polynomials have chances of being semiplanar

The reason DO polynomials have better chances than other polynomials rests on two facts:

Why DO polynomials have chances of being semiplanar

The reason DO polynomials have better chances than other polynomials rests on two facts:

- ⊕ Linear operators (linearized polynomials) are always regular on their image sets – they are necessarily p^k-to-1 for some k, where p is the characteristic.

Why DO polynomials have chances of being semiplanar

The reason DO polynomials have better chances than other polynomials rests on two facts:

- ⊕ Linear operators (linearized polynomials) are always regular on their image sets – they are necessarily p^k-to-1 for some k, where p is the characteristic.
- ⊕ DO polynomials are precisely those polynomials whose derivatives are linear operators.

Why DO polynomials have chances of being semiplanar

The reason DO polynomials have better chances than other polynomials rests on two facts:

- $\oplus$ Linear operators (linearized polynomials) are always regular on their image sets – they are necessarily p^k-to-1 for some k, where p is the characteristic.
- $\oplus$ DO polynomials are precisely those polynomials whose derivatives are linear operators.

So the derivative of a DO polynomial in the direction a will always have 0 or p^{k_a} solutions to $f(x+a) - f(x) = b$ for each b, where k_a is only dependent on a.

Why DO polynomials have chances of being semiplanar

The reason DO polynomials have better chances than other polynomials rests on two facts:

- Linear operators (linearized polynomials) are always regular on their image sets – they are necessarily p^k-to-1 for some k, where p is the characteristic.
- DO polynomials are precisely those polynomials whose derivatives are linear operators.

So the derivative of a DO polynomial in the direction a will always have 0 or p^{k_a} solutions to $f(x+a) - f(x) = b$ for each b, where k_a is only dependent on a.

Thus, the only requirement is that all the k_a are the same – the regularity of preimages is already taken care of.

And DO monomials have to be planar or semiplanar

The derivative of a DO polynomial in the direction a will always have 0 or p^{k_a} solutions to $f(x+a) - f(x) = b$ for each b.

And DO monomials have to be planar or semiplanar

The derivative of a DO polynomial in the direction a will always have 0 or p^{k_a} solutions to $f(x+a) - f(x) = b$ for each b.

But for monomials, all the derivatives are basically equivalent.

$$\begin{aligned}(x+a)^n - x^n &= a^n((x/a)+1)^n - x^n \\ &= a^n((y+1)^n - y^n) \text{ for } y = x/a.\end{aligned}$$

This means all the derivatives have the same multiplicities of preimages, just for different images.

And DO monomials have to be planar or semiplanar

The derivative of a DO polynomial in the direction a will always have 0 or p^{k_a} solutions to $f(x+a) - f(x) = b$ for each b.

But for monomials, all the derivatives are basically equivalent.

$$\begin{aligned}(x+a)^n - x^n &= a^n((x/a)+1)^n - x^n \\ &= a^n((y+1)^n - y^n) \text{ for } y = x/a.\end{aligned}$$

This means all the derivatives have the same multiplicities of preimages, just for different images.

So for DO monomials, all the derivatives have a regularity of preimages because they're DOs, and the same multiplicities of preimages because they're monomials.

That means DO monomials *have to be planar or semiplanar!*

Composing planar functions with linear transformations

Theorem (Coulter & Matthews, 1997)
Let $f, L \in \mathbb{F}_q[x]$ with L a linearized polynomial.
The following are equivalent.

(i) $f(L)$ is planar.

(ii) $L(f)$ is planar.

(iii) f is planar and L is a permutation polynomial.

Composing planar functions with linear transformations

Theorem (Coulter & Matthews, 1997)
Let $f, L \in \mathbb{F}_q[x]$ with L a linearized polynomial.
The following are equivalent.

(i) $f(L)$ is planar.

(ii) $L(f)$ is planar.

(iii) f is planar and L is a permutation polynomial.

This looks like a version of...

Definition (Not sure who did this first!)
Let $f, h \in \mathbb{F}_q[x]$. Then we say f and h are *extended affine equivalent* if there exists linearized L_1, L_2, L_3, with L_1, L_2 permutations, and constants c_1, c_2 such that

$$f(x) \equiv L_2(h(L_1(x) + c_1)) + L_3(x) + c_2 \bmod (x^q - x).$$

APN/semiplanar equivalent?

APN/semiplanar equivalent?

But it is not!

APN/semiplanar equivalent?

An equivalent result to the Coulter/Matthews statement would be:

A Theorem

Let $f, L \in \mathbb{F}_q[x]$ with L a linearized polynomial.
The following are equivalent.

(i) $f(L)$ is semiplanar of index λ.

(ii) $L(f)$ is semiplanar of index λ.

(iii) f is semiplanar of index λ and L is a permutation polynomial.

An equivalent result to the Coulter/Matthews statement would be:

A Theorem this is not
Let $f, L \in \mathbb{F}_q[x]$ with L a linearized polynomial.
The following are equivalent.

(i) $f(L)$ is semiplanar of index λ.

(ii) $L(f)$ is semiplanar of index λ.

(iii) f is semiplanar of index λ and L is a permutation polynomial.

But this is not true in general!

APN/semiplanar equivalent?

In fact, I don't even know if this works for $\lambda = 2$/APN...

A Theorem?
Let $f, L \in \mathbb{F}_q[x]$ with L a linearized polynomial.
The following are equivalent.

(i) $f(L)$ is APN.

(ii) $L(f)$ is APN.

(iii) f is APN and L is a permutation polynomial.

APN/semiplanar equivalent?

In fact, I don't even know if this works for $\lambda = 2$/APN...

A Theorem?

Let $f, L \in \mathbb{F}_q[x]$ with L a linearized polynomial.
The following are equivalent.

(i) $f(L)$ is APN.

(ii) $L(f)$ is APN.

(iii) f is APN and L is a permutation polynomial.

In a very quick search, I couldn't find a result stating this explicitly, and I suspect it is probably false.

So what do we have?

Theorem (Coulter & Matthews, 1997)
Let $f, L \in \mathbb{F}_q[x]$ with L a linearized polynomial.
The following are equivalent.

(i) $f(L)$ is planar.
(ii) $L(f)$ is planar.
(iii) f is planar and L is a permutation polynomial.

What we have from EA-equivalence is an equivalence relation defined on functions using linear transformations which preserves semiplanarity.

But it doesn't force the decomposition conclusion we see in this planarity theorem.

Specifically, if I give you a polynomial $L(f)$ which is semiplanar of index λ, then you cannot conclude L is a permutation polynomial and f is semiplanar of index λ.

So the equivalence of the 3 statements fails.

Semiplanar functions and linear transformations

Theorem (Coulter & Fain, 2021)
Let $f, L \in \mathbb{F}_q[x]$ with L a linearized polynomial.
The following are equivalent.

(i) $f(L)$ is semiplanar of index λ.

(ii) f is semiplanar of index λ and L is a permutation polynomial.

Thus, you cannot relax the condition with regards to inner composition.

Semiplanar functions and linear transformations

Theorem (Coulter & Fain, 2021)
Let $f, L \in \mathbb{F}_q[x]$ with L a linearized polynomial.
The following are equivalent.

(i) $f(L)$ is semiplanar of index λ.

(ii) f is semiplanar of index λ and L is a permutation polynomial.

Thus, you cannot relax the condition with regards to inner composition.

But outer compositions do not behave as nicely.

Semiplanar functions and linear transformations

Lemma (Coulter & Fain, 2021)
Let $f, L, M \in \mathbb{F}_q[x]$ with f planar and L, M linearized polynomials.

(i) $L(f)$ is semiplanar of index $\# \ker(L)$.

(ii) $M(L(f))$ is either semiplanar of index $\# \ker(M(L))$ or $M(L(f(x))) \equiv 0 \bmod (x^q - x)$.

Semiplanar functions and linear transformations

Lemma (Coulter & Fain, 2021)
Let $f, L, M \in \mathbb{F}_q[x]$ with f planar and L, M linearized polynomials.

(i) $L(f)$ is semiplanar of index $\#\ker(L)$.

(ii) $M(L(f))$ is either semiplanar of index $\#\ker(M(L))$ or $M(L(f(x))) \equiv 0 \bmod (x^q - x)$.

Lemma (Coulter & Fain, 2021)
Let $f, L \in \mathbb{F}_q[x]$ with f semiplanar of some index $\lambda \geq 2$ and L a linearized polynomial.
Then $L(f)$ is semiplanar of some index or equivalent to the 0 polynomial if and only if $\#(\ker(L) \cap \operatorname{Im}(\Delta_{f,a}))$ is the same for all $a \in \mathbb{F}_q^\star$.
Here $\Delta_{f,a}(x) = f(x+a) - f(x) - f(a)$.

Open problems and future work

Open problems and future work

- Construct semiplanar functions over non-abelian groups or prove they don't exist.

Open problems and future work

- Construct semiplanar functions over non-abelian groups or prove they don't exist.
- Construct semiplanar functions over abelian groups that are not elementary abelian p-groups, or prove they don't exist.

Open problems and future work

- Construct semiplanar functions over non-abelian groups or prove they don't exist.
- Construct semiplanar functions over abelian groups that are not elementary abelian p-groups, or prove they don't exist.
- Conjecture: Over odd finite fields, all semiplanar functions of index $\lambda > 1$ are EA-equivalent to DO polynomials.

Open problems and future work

- Construct semiplanar functions over non-abelian groups or prove they don't exist.
- Construct semiplanar functions over abelian groups that are not elementary abelian p-groups, or prove they don't exist.
- Conjecture: Over odd finite fields, all semiplanar functions of index $\lambda > 1$ are EA-equivalent to DO polynomials.
- Classify semiplanar monomials.

Open problems and future work

- Construct semiplanar functions over non-abelian groups or prove they don't exist.
- Construct semiplanar functions over abelian groups that are not elementary abelian p-groups, or prove they don't exist.
- Conjecture: Over odd finite fields, all semiplanar functions of index $\lambda > 1$ are EA-equivalent to DO polynomials.
- Classify semiplanar monomials.
- Obtain a better understanding of how composition of semiplanar functions and linear transformations behaves.

Open problems and future work

- $\oplus$ Construct semiplanar functions over non-abelian groups or prove they don't exist.
- $\oplus$ Construct semiplanar functions over abelian groups that are not elementary abelian p-groups, or prove they don't exist.
- $\oplus$ Conjecture: Over odd finite fields, all semiplanar functions of index $\lambda > 1$ are EA-equivalent to DO polynomials.
- $\oplus$ Classify semiplanar monomials.
- $\oplus$ Obtain a better understanding of how composition of semiplanar functions and linear transformations behaves.
- $\oplus$ We've done very little so far on investigating automorphism groups of SSDs. The semibiplane case, in particular, needs to be looked at.

Fifth Part

The end.