Cyclic line-spreads and linear spaces

Finite Geometries 2022

Cian Jameson
(joint work with John Sheekey)

University College Dublin

Introduction

Consider the incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ where the point $x \in \mathcal{P}$ is on the line $\ell \in \mathcal{L}$ if $(x, \ell) \in \mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$.

Introduction

Consider the incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ where the point $x \in \mathcal{P}$ is on the line $\ell \in \mathcal{L}$ if $(x, \ell) \in \mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$.

If

- every line contains at least two points;
- every pair of distinct points lie on a unique line;
- every pair of distinct lines meet in at most one common point,

then $\mathcal{S}$ is a *linear space*.

Introduction

Consider the incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ where the point $x \in \mathcal{P}$ is on the line $\ell \in \mathcal{L}$ if $(x, \ell) \in \mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$.

If

- every line contains at least two points;
- every pair of distinct points lie on a unique line;
- every pair of distinct lines meet in at most one common point,

then $\mathcal{S}$ is a *linear space*.

Example

Consider the finite field $\mathbb{F}_q$. Let $\mathcal{P} = \{v \in \mathbb{F}_q^n\}$, let $\mathcal{L} = \{u + \langle v \rangle : u, v \in \mathbb{F}_q^n\}$ and let $(x, \ell) \in \mathcal{I} \iff x \in \ell$. Then $(\mathcal{P}, \mathcal{L}, \mathcal{I}) =: \mathrm{AG}(n, q)$ is a linear space.

Linear spaces

An *automorphism* of a linear space L is a type- and incidence-preserving bijection on L.

Linear spaces

An *automorphism* of a linear space L is a type- and incidence-preserving bijection on L.

The set of automorphisms of L forms a group under composition, called the *automorphism group* of L, and is denoted by $\mathrm{Aut}(L)$.

Linear spaces

An *automorphism* of a linear space L is a type- and incidence-preserving bijection on L.

The set of automorphisms of L forms a group under composition, called the *automorphism group* of L, and is denoted by $\mathrm{Aut}(L)$.

Example

Let $L = \mathrm{AG}(n, q)$ be the linear space in the previous example. Then it is known that

$$\begin{aligned} \mathrm{Aut}(L) &= (\text{Translations}) \circ (\text{Invertible semilinear transformations}) \\ &= \{T : T(v) = Av^{\sigma} + u\} \\ &= \mathrm{A\Gamma L}(n, q). \end{aligned}$$

Linear spaces

Example

Let $L = \mathrm{AG}(n, q)$. Then $\mathsf{Aut}(L)$ acts transitively on

- points of L,
- pairs of points of L,
- pairs of nonincident lines of L,
- flags of L ...

Linear spaces

Example

Let $L = \mathrm{AG}(n, q)$. Then $\mathrm{Aut}(L)$ acts transitively on

- points of L,
- pairs of points of L,
- pairs of nonincident lines of L,
- flags of L ...

A *flag* of L is an incident point-line pair (x, ℓ).

Linear spaces

Question: For which linear spaces L does $\mathrm{Aut}(L)$ act transitively on points, lines, pairs of points, pairs of lines, flags, etc.?

Linear spaces

Question: For which linear spaces L does $\mathrm{Aut}(L)$ act transitively on points, lines, pairs of points, pairs of lines, flags, etc.?

In particular, when is $\mathrm{Aut}(L)$ **flag-transitive**?

Linear spaces

Question: For which linear spaces L does $\mathrm{Aut}(L)$ act transitively on points, lines, pairs of points, pairs of lines, flags, etc.?

In particular, when is $\mathrm{Aut}(L)$ **flag-transitive**?

Due to work by Buekenhout, Delandtsheer, Doyen et al. (1990), Liebeck (1998), Saxl (2002) and others, the result is known for all L and $\mathrm{Aut}(L)$ except when L is constructed from a spread.

Spreads

Let $V(n, q)$ denote an n-dimensional vector space over $\mathbb{F}_q$.

Spreads

Let $V(n,q)$ denote an n-dimensional vector space over $\mathbb{F}_q$.

Spreads

A *t-spread* of $V(n,q)$ is a set S of t-dimensional subspaces of $V(n,q)$ such that every nonzero vector of $V(n,q)$ is contained in exactly one element of S.

Spreads

Let $V(n,q)$ denote an n-dimensional vector space over $\mathbb{F}_q$.

Spreads

A *t-spread* of $V(n,q)$ is a set S of t-dimensional subspaces of $V(n,q)$ such that every nonzero vector of $V(n,q)$ is contained in exactly one element of S.

Hence
$$|S| = \frac{q^n - 1}{q^t - 1}.$$

Spreads

Let $V(n,q)$ denote an n-dimensional vector space over $\mathbb{F}_q$.

Spreads

A *t-spread* of $V(n,q)$ is a set S of t-dimensional subspaces of $V(n,q)$ such that every nonzero vector of $V(n,q)$ is contained in exactly one element of S.

Hence

$$|S| = \frac{q^n - 1}{q^t - 1}.$$

- It is known (due to Segre) that t-spreads exist in $V(n,q)$ if and only if t divides n.

Spreads

Let $V(n, q)$ denote an n-dimensional vector space over $\mathbb{F}_q$.

Spreads

A *t-spread* of $V(n, q)$ is a set S of t-dimensional subspaces of $V(n, q)$ such that every nonzero vector of $V(n, q)$ is contained in exactly one element of S.

Hence

$$|S| = \frac{q^n - 1}{q^t - 1}.$$

- It is known (due to Segre) that t-spreads exist in $V(n, q)$ if and only if t divides n.
- Equivalently we could consider $(t-1)$-spreads in $\mathrm{PG}(n-1, q)$.

Spreads

Example (Desarguesian spread)

Consider $\mathbb{F}_{q^{tm}}$ as a tm-dimensional vector space over $\mathbb{F}_q$. Then

$$S = \{\{ax : x \in \mathbb{F}_{q^t}\} : a \in \mathbb{F}_{q^{tm}}^{\times}\}$$

is a t-spread of $\mathbb{F}_{q^{tm}} \cong V(tm, q)$.

Linear space from a spread

Let S be a t-spread of $V = V(n,q)$. Let $\mathcal{P} = \{v \in V\}$, let $\mathcal{L} = \{u + U : u \in V, U \in S\}$ and let $(x,\ell) \in \mathcal{I} \iff x \in \ell$. Then $(\mathcal{P},\mathcal{L},\mathcal{I})$ is a linear space. We will refer to a linear space constructed in this way from a t-spread S as $L(S)$ and say it is *associated* with S.

Linear space from a spread

Let S be a t-spread of $V = V(n, q)$. Let $\mathcal{P} = \{v \in V\}$, let $\mathcal{L} = \{u + U : u \in V, U \in S\}$ and let $(x, \ell) \in \mathcal{I} \iff x \in \ell$. Then $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ is a linear space. We will refer to a linear space constructed in this way from a t-spread S as $L(S)$ and say it is *associated* with S.

This coincides with the *Barlotti-Cofman* construction for linear spaces; specifically *translation Sperner spaces*. When $n = 2t$ this becomes the *André/Bruck-Bose* construction for affine (and projective) planes.

Linear space from a spread

Let S be a t-spread of $V = V(n,q)$. Let $\mathcal{P} = \{v \in V\}$, let $\mathcal{L} = \{u + U : u \in V, U \in S\}$ and let $(x,\ell) \in \mathcal{I} \iff x \in \ell$. Then $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ is a linear space. We will refer to a linear space constructed in this way from a t-spread S as $L(S)$ and say it is *associated* with S.

This coincides with the *Barlotti-Cofman* construction for linear spaces; specifically *translation Sperner spaces*. When $n = 2t$ this becomes the *André/Bruck-Bose* construction for affine (and projective) planes.

The linear space associated with the Desarguesian t-spread in $V(mt,q)$ is $\mathrm{AG}(m,q^t)$.

Linear space from a spread

Let $L(S)$ be a linear space associated with a t-spread S of $V(n,q)$. Then it is known that

$$\begin{aligned}\mathrm{Aut}(L(S)) &= (\text{Translations}) \circ (\text{Semilinear transformations stabilizing } S)\\ &= T \circ G_0.\end{aligned}$$

Here $G_0 \leq \Gamma\mathrm{L}(n,q)$.

Linear space from a spread

Let $L(S)$ be a linear space associated with a t-spread S of $V(n, q)$. Then it is known that

$$\begin{aligned} \mathrm{Aut}(L(S)) &= (\text{Translations}) \circ (\text{Semilinear transformations stabilizing } S) \\ &= T \circ G_0. \end{aligned}$$

Here $G_0 \leq \Gamma\mathrm{L}(n, q)$.

$\mathrm{Aut}(L(S))$ is transitive on points. It is transitive on flags if and only if G_0 is transitive on the elements of the spread.

Linear spaces

Question: For which linear spaces L does $\mathrm{Aut}(L)$ act transitively on points, lines, pairs of points, pairs of lines, flags, etc.?

Linear spaces

Question: For which linear spaces L does $\mathrm{Aut}(L)$ act transitively on points, lines, pairs of points, pairs of lines, flags, etc.?

In particular, when is $\mathrm{Aut}(L)$ **flag-transitive**?

Linear spaces

Question: For which linear spaces L does $\mathrm{Aut}(L)$ act transitively on points, lines, pairs of points, pairs of lines, flags, etc.?

In particular, when is $\mathrm{Aut}(L)$ **flag-transitive**?

Due to work by Buekenhout, Delandtsheer, Doyen et al. (1990), Liebeck (1998), Saxl (2002) and others, the result is known for all L and $\mathrm{Aut}(L)$ except when L is constructed from a t-spread of $V(n, q)$ and $\mathrm{Aut}(L)$ is $T \circ G_0$, where G_0 is a subgroup of $\Gamma\mathrm{L}(1, q^n) \leq \Gamma\mathrm{L}(n, q)$.

Linear spaces

Question: For which linear spaces L does $\mathrm{Aut}(L)$ act transitively on points, lines, pairs of points, pairs of lines, flags, etc.?

In particular, when is $\mathrm{Aut}(L)$ **flag-transitive**?

Due to work by Buekenhout, Delandtsheer, Doyen et al. (1990), Liebeck (1998), Saxl (2002) and others, the result is known for all L and $\mathrm{Aut}(L)$ except when L is constructed from a t-spread of $V(n,q)$ and $\mathrm{Aut}(L)$ is $T \circ G_0$, where G_0 is a subgroup of $\Gamma\mathrm{L}(1,q^n) \leq \Gamma\mathrm{L}(n,q)$.

$$\Gamma\mathrm{L}(1,q^n) = \{x \mapsto ax^{\sigma} : a \in \mathbb{F}_{q^n}^{\times}, \sigma \in \mathrm{Aut}(\mathbb{F}_{q^n})\}$$

Line-spreads

Pauley and Bamberg (2007) studied the case $t = 2$ and $G_0 = C := \left\langle \omega^{q+1} \right\rangle \leq \Gamma\mathrm{L}(1, q^{2m})$, where ω is a generator of $\mathbb{F}_{q^{2m}}^{\times}$.

Line-spreads

Pauley and Bamberg (2007) studied the case $t = 2$ and $G_0 = C := \langle \omega^{q+1} \rangle \leq \Gamma\mathrm{L}(1, q^{2m})$, where ω is a generator of $\mathbb{F}_{q^{2m}}^{\times}$.

We call a 2-spread with G_0 cyclic a *cyclic 2-spread*, or a *cyclic line-spread* in $\mathrm{PG}(2m-1, q)$.

Line-spreads

Pauley and Bamberg (2007) studied the case $t = 2$ and $G_0 = C := \langle \omega^{q+1} \rangle \leq \Gamma\mathrm{L}(1, q^{2m})$, where ω is a generator of $\mathbb{F}_{q^{2m}}^{\times}$.

We call a 2-spread with G_0 cyclic a *cyclic 2-spread*, or a *cyclic line-spread* in $\mathrm{PG}(2m-1, q)$.

They showed that every such spread was equivalent to one of the form

$$S_b = \{\{a(x - bx^q) : x \in \mathbb{F}_{q^2}\} : a \in C\},$$

and found criteria for when this forms a spread in terms of the minimal polynomial $P(x)$ of b.

Line-spreads

Theorem (Pauley-Bamberg, 2007)

Let $P(x)$ be an irreducible polynomial over $\mathbb{F}_{q^2}$ of degree m and let b be a root of $P(x)$. Then S_b is a cyclic 2-spread if and only if for all nonzero $x, y \in \mathbb{F}_{q^2}$ we have that

$$\frac{x^m P(x^{q-1})}{y^m P(y^{q-1})} \in \mathbb{F}_q \implies \frac{x}{y} \in \mathbb{F}_q. \quad (\star)$$

Line-spreads

Theorem (Pauley-Bamberg, 2007)

Let $P(x)$ be an irreducible polynomial over $\mathbb{F}_{q^2}$ of degree m and let b be a root of $P(x)$. Then S_b is a cyclic 2-spread if and only if for all nonzero $x, y \in \mathbb{F}_{q^2}$ we have that

$$\frac{x^m P(x^{q-1})}{y^m P(y^{q-1})} \in \mathbb{F}_q \implies \frac{x}{y} \in \mathbb{F}_q. \quad (\star)$$

As they also showed that different roots of the same polynomial define equivalent spreads, we abuse notation a bit and refer to such a spread as S_P.

Theorem (Pauley-Bamberg, 2007)

Let $P(x), Q(x) \in \mathbb{F}_{q^2}[x]$ satisfy $\star$. Then S_P and S_Q are equivalent if and only if

$$P(x) = \lambda(u + v^q x)^m Q^\sigma \left(\frac{v + u^q x}{u + v^q x}\right)$$

for some $u, v, \lambda \in \mathbb{F}_{q^2}$ where $\lambda \neq 0$ and $u^{q+1} \neq v^{q+1}$.

Known constructions

- Desarguesian spread.
- Kantor (1993): $P(x) = x^m - \zeta$, where ζ is a generator of $\mathbb{F}_{q^2}^\times$.
- Bamberg and Pauley (2007): $P(x) = \frac{x^{p+1}-1}{x-1} - 2$ where p is an odd prime.
- Feng and Lu (2021):

$$g_n(x) := \frac{(\delta x - 1)^n - \delta(x-\delta)^n}{\delta^n - \delta}$$

where $d > 1$ is an odd divisor of $q+1$, u is a proper divisor of d, $t \in \mathbb{N}^+$, $n = d^t u$ and $\delta \in \mathbb{F}_{q^2}^\times$ is an element of order $q+1$.

Binomials

Theorem

The polynomial $P(x) = x^m - \theta$ is irreducible in $\mathbb{F}_{q^2}[x]$ and satisfies $\star$ if and only if the following hold:

(i) every prime factor of m divides $o(\theta)$ but not $\frac{q^2-1}{o(\theta)}$;

(ii) $(m, q+1) = 1$.

Binomials

Theorem

The polynomial $P(x) = x^m - \theta$ is irreducible in $\mathbb{F}_{q^2}[x]$ and satisfies $\star$ if and only if the following hold:

(i) every prime factor of m divides $o(\theta)$ but not $\frac{q^2-1}{o(\theta)}$;

(ii) $(m, q+1) = 1$.

In particular, if $m = 3$ then there exists an irreducible cubic binomial satisfying $\star$ if and only if $q \equiv 1 \mod 3$.

Binomials

Theorem

The polynomial $P(x) = x^m - \theta$ is irreducible in $\mathbb{F}_{q^2}[x]$ and satisfies $\star$ if and only if the following hold:

(i) every prime factor of m divides $o(\theta)$ but not $\frac{q^2-1}{o(\theta)}$;

(ii) $(m, q+1) = 1$.

In particular, if $m = 3$ then there exists an irreducible cubic binomial satisfying $\star$ if and only if $q \equiv 1 \mod 3$.

We also calculated the equivalence classes of binomials for arbitrary degree.

An equivalent critieron

Let $P(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{F}_{q^2}[x]$, and define $\tilde{P}(x) := \sum_{i=0}^{m} a_{m-i}^{q} x^i$.

An equivalent critieron

Let $P(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{F}_{q^2}[x]$, and define $\tilde{P}(x) := \sum_{i=0}^{m} a_{m-i}^{q} x^i$. We define a polynomial in two variables as follows.

$$H_P(z, w) := \frac{P(z)\tilde{P}(w) - \tilde{P}(z)P(w)}{z - w}.$$

An equivalent critieron

Let $P(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{F}_{q^2}[x]$, and define $\tilde{P}(x) := \sum_{i=0}^{m} a_{m-i}^q x^i$. We define a polynomial in two variables as follows.

$$H_P(z, w) := \frac{P(z)\tilde{P}(w) - \tilde{P}(z)P(w)}{z - w}.$$

Lemma

A polynomial $P(x)$ satisfies $\star \iff$ the system $H_P(z, w) = 0$, $z^{q+1} = w^{q+1} = 1$ has no solutions with $z \neq w$.

The case $m = 3$

Goal

- To classify all cyclic 2-spreads in $V(6, q)$.

The case $m = 3$

Goal

- To classify all cyclic 2-spreads in $V(6, q)$.
- This is the smallest open case; the case $m = 2$ is fully understood.

The case $m = 3$

Goal

- To classify all cyclic 2-spreads in $V(6, q)$.
- This is the smallest open case; the case $m = 2$ is fully understood.
- In this case, $H_P(z, w)$ has degree two in both variables.

The case $m = 3$

Goal

- To classify all cyclic 2-spreads in $V(6, q)$.
- This is the smallest open case; the case $m = 2$ is fully understood.
- In this case, $H_P(z, w)$ has degree two in both variables.
- We analyse the case where $H_P(z, w)$ is reducible.

The case $m = 3$

Goal

- To classify all cyclic 2-spreads in $V(6, q)$.
- This is the smallest open case; the case $m = 2$ is fully understood.
- In this case, $H_P(z, w)$ has degree two in both variables.
- We analyse the case where $H_P(z, w)$ is reducible.
- For technical reasons we restrict to q neither a power of 2 nor 3.

The case $m = 3$

If $H_P(z, w)$ is reducible, then either

$$H_P(z, w) = \lambda(czw + az + bw + d)(czw + bz + aw + d)$$

or

$$H_P(z, w) = \lambda(czw + a(z + w) + d)(c'zw + b(z + w) + d').$$

The case $m = 3$

If $H_P(z, w)$ is reducible, then ~~either~~

$$H_P(z, w) = \lambda(czw + az + bw + d)(czw + bz + aw + d)$$

~~or~~

$$\cancel{H_P(z, w) = \lambda(czw + a(z + w) + d)(c'zw + b(z + w) + d')}.$$

The case $m = 3$

If $H_P(z, w)$ is reducible, then ~~either~~

$$H_P(z, w) = \lambda(czw + az + bw + d)(czw + bz + aw + d)$$

~~or~~

$$\cancel{H_P(z, w) = \lambda(czw + a(z + w) + d)(c'zw + b(z + w) + d')}.$$

Let $P(x) = x^3 - \delta x^2 - \gamma x - \theta \in \mathbb{F}_{q^2}[x]$. Then

$$\begin{aligned} H_P(z, w) = &(\theta^q \delta + \gamma^q) z^2 w^2 + (\theta^q \gamma + \delta^q)(z^2 w + z w^2) \\ &+ (\theta^{q+1} - 1)(z^2 + zw + w^2) + (\gamma^{q+1} - \delta^{q+1}) zw \\ &+ (\theta \gamma^q + \delta)(z + w) + (\theta \delta^q + \gamma). \end{aligned}$$

The case $m = 3$

Example

Let $P(x) = x^3 - \delta x^2 - (\delta + 3)x - 1$. Then

$$H_P(z, w) = (zw + z + 1)(zw + w + 1).$$

The case $m = 3$

Example

Let $P(x) = x^3 - \delta x^2 - (\delta + 3)x - 1$. Then

$$H_P(z, w) = (zw + z + 1)(zw + w + 1).$$

Suppose $zw + z + 1 = 0 \iff z = \frac{-1}{w+1}$.

The case $m = 3$

Example

Let $P(x) = x^3 - \delta x^2 - (\delta + 3)x - 1$. Then

$$H_P(z, w) = (zw + z + 1)(zw + w + 1).$$

Suppose $zw + z + 1 = 0 \iff z = \frac{-1}{w+1}$. Then

$$\begin{aligned} & z^{q+1} = 1 = w^{q+1} \\ \iff & w^{q+1} + w^q + w = 0 \\ \iff & w^2 + w + 1 = 0 \\ \iff & z = w. \end{aligned}$$

The case $m = 3$

Example

Let $P(x) = x^3 - \delta x^2 - (\delta + 3)x - 1$. Then

$$H_P(z, w) = (zw + z + 1)(zw + w + 1).$$

Suppose $zw + z + 1 = 0 \iff z = \frac{-1}{w+1}$. Then

$$\begin{aligned} & z^{q+1} = 1 = w^{q+1} \\ \iff & w^{q+1} + w^q + w = 0 \\ \iff & w^2 + w + 1 = 0 \\ \iff & z = w. \end{aligned}$$

Hence $P(x)$ satisfies $\star$.

The case $m = 3$

Theorem

Let $P(x) = x^3 - \delta x^2 - \gamma x - \theta \in \mathbb{F}_{q^2}[x]$. Then $H_P(z,w)$ is reducible (and not identically zero) if and only if one of the following holds:

(i) $P(x) = B_\theta(x) := x^3 - \theta$;

(ii) $P(x) = P_{\delta,\alpha}(x) := x^3 - \delta x^2 - (\delta\alpha + 3\alpha^{1-q})x - (\delta\alpha^2\left(\frac{1-\alpha^{-(q+1)}}{3}\right) + \alpha^{2-q})$, $\alpha \neq 0$;

(iii) $P(x) = Q_{\delta,\gamma}(x) := x^3 - \delta x^2 - \gamma x + \delta\gamma/9$, $\gamma^{q+1} = 9$.

Furthermore

- an irreducible $P_{\delta,\alpha}(x)$ satisfies $\star$ if and only if $\frac{4-\alpha^{q+1}}{3\alpha^{q+1}}$ is a nonzero square in $\mathbb{F}_q$, and $\delta = 0$ or $(\alpha + 3\delta^{-q})^{q+1} \neq 1$;.
- an irreducible $Q_{\delta,\gamma}(x)$ satisfies $\star$ if and only if $\gamma^{\frac{q+1}{2}} = 3$.

The case $m = 3$

Theorem

Let $P(x)$ be an irreducible polynomial of the form $B_\theta(x)$, $P_{\delta,\alpha}(x)$ or $Q_{\delta,\gamma}(x)$ that satisfies $\star$. Then $P(x)$ is equivalent to some $P_{\delta',1}(x)$.

The case $m = 3$

Theorem

Let $P(x)$ be an irreducible polynomial of the form $B_\theta(x)$, $P_{\delta,\alpha}(x)$ or $Q_{\delta,\gamma}(x)$ that satisfies $\star$. Then $P(x)$ is equivalent to some $P_{\delta',1}(x)$.

By counting the number of irreducibles of the form $P_{\delta,1}(x)$, and calculating precisely the equivalences between polynomials of this form, we get the following.

The case $m = 3$

Theorem

Let $P(x)$ be an irreducible polynomial of the form $B_\theta(x)$, $P_{\delta,\alpha}(x)$ or $Q_{\delta,\gamma}(x)$ that satisfies $\star$. Then $P(x)$ is equivalent to some $P_{\delta',1}(x)$.

By counting the number of irreducibles of the form $P_{\delta,1}(x)$, and calculating precisely the equivalences between polynomials of this form, we get the following.

Theorem

The number of equivalence classes of irreducible cubic polynomials satisfying $\star$ such that $H_P(z,w)$ is reducible is precisely

$$\begin{cases} \frac{q-1}{3}, & \text{if } q \equiv 1 \mod 3 \\ \frac{q+1}{3}, & \text{if } q \not\equiv 1 \mod 3 \end{cases}.$$

The case $m = 3$

Given a $P_{\delta,1}(x)$ satisfying $\star$, the set of values of δ' for which $P_{\delta,1}(x)$ is equivalent to $P_{\delta',1}(x)$ is

$$D = \left\{ \frac{-3(w^3 - 3w^2 + 1) - \delta(w^3 - 3w + 1)}{w^3 - 3w + 1 + \delta w(w-1)} : w^{q+1} = 1 \right\}$$
$$\cup \left\{ \frac{9w(w-1) + \delta(w^3 - 3w + 1)}{w^3 - 3w^2 + 1 - \delta w(w-1)} : w^{q+1} = 1 \right\}.$$

Counts

	$\#\ B_\theta\ (q \equiv 1 \bmod 3)$	$\#\ P_{\delta,\alpha}$	$\#\ Q_{\delta,\gamma}$	$\#\ P_{\delta,1}$
Total	q^2	$(q^2-1)^2$	$\frac{q^2(q+1)}{2}$	q^2
Reducible	$\frac{q^2+2}{3}$	$\frac{(q-1)(q+1)^3}{3}$	$\frac{(q+1)(q^2+2)}{6}$	$\frac{q^2+2}{3}$
Irreducible	$\frac{2(q^2-1)}{3}$	$\frac{2(q-2)(q-1)(q+1)^2}{3}$	$\frac{(q-1)(q+1)^2}{3}$	$\frac{2(q^2-1)}{3}$

Since

$$|D| = \begin{cases} 2(q+1), & \text{if } q \equiv 1 \mod 3 \\ 2(q-1), & \text{if } q \not\equiv 1 \mod 3 \end{cases},$$

the number of equivalence classes is

$$\begin{cases} \frac{q-1}{3}, & \text{if } q \equiv 1 \mod 3 \\ \frac{q+1}{3}, & \text{if } q \not\equiv 1 \mod 3 \end{cases}.$$

Remarks

We have

$$(H_P(z,w) \text{ reducible and conditions}) \implies \star.$$

Remarks

We have

$$(H_P(z,w) \text{ reducible and conditions}) \implies \star.$$

We believe

$$H_P(z,w) \text{ irreducible} \implies \neg\star\,.$$

Remarks

In their work on characterising permutation polynomials of $\mathbb{F}_{q^2}$ of the form

$$f_{a,b}(X) = X(1 + aX^{q(q-1)} + bX^{2(q-1)}),$$

Bartoli and Timpanella (2021) considered a curve with affine equation

$$-b^{q+1} H_P(z, w) = 0$$

where $P(x) = x^3 + b^{-1}x + ab^{-1}$. They showed that $f_{a,b}(X)$ is a PP if and only if $\star$ is satisfied. It follows that $P(x)$ is of the form $P_{\delta,\alpha}(x)$ with $\delta = 0$, $a = \alpha/3$ and $b = -\alpha^{q-1}/3$.

Remarks

Applying methods of Stichtenoth-Topuzoğlu (2012) and Gow-McGuire (2021) tells us that every irreducible cubic factor of $(x^{q^2+1} + x^{q^2} + 1)(x^{q^2+1} + x + 1) \in \mathbb{F}_{q^2}[x]$ is of the form

$$P_{\delta,1}(x) = x^3 - \delta x^2 - (\delta + 3)x - 1.$$

Remarks

Applying methods of Stichtenoth-Topuzoğlu (2012) and Gow-McGuire (2021) tells us that every irreducible cubic factor of $(x^{q^2+1} + x^{q^2} + 1)(x^{q^2+1} + x + 1) \in \mathbb{F}_{q^2}[x]$ is of the form

$$P_{\delta,1}(x) = x^3 - \delta x^2 - (\delta + 3)x - 1.$$

We hope to exploit this connection to find polynomials of other degrees satisfying $\star$.

Remarks

Feng and Lu (2021) showed that

$$g_n(x) := \frac{(\delta x - 1)^n - \delta(x - \delta)^n}{\delta^n - \delta}$$

satisfies $\star$, where $d > 1$ is an odd divisor of $q + 1$, u is a proper divisor of d, $t \in \mathbb{N}^+$, $n = d^t u$ and $\delta \in \mathbb{F}_{q^2}^{\times}$ is an element of order $q + 1$.

Remarks

Feng and Lu (2021) showed that

$$g_n(x) \coloneqq \frac{(\delta x - 1)^n - \delta(x-\delta)^n}{\delta^n - \delta}$$

satisfies $\star$, where $d > 1$ is an odd divisor of $q+1$, u is a proper divisor of d, $t \in \mathbb{N}^+$, $n = d^t u$ and $\delta \in \mathbb{F}_{q^2}^\times$ is an element of order $q+1$.

We have

$$g_3(x) = P_{0,-(\delta+\delta^{-1})}(x) \in \mathbb{F}_q[x].$$

Not every irreducible satisfying $\star$ is equivalent to one of the form $g_3(x)$, and so this construction is a proper subset of ours for the case $m = 3$.

Thank you for your attention!

Equivalence between $P_{0,\alpha}$ and a general cubic

A polynomial of the form $P_{0,\alpha}$ is equivalent to $x^3 - \delta x^2 - \gamma x - \theta \in \mathbb{F}_{q^2}[x]$ if and only if the following hold for some $u, v \in \mathbb{F}_{q^2}$ with $u^{q+1} \neq v^{q+1}$:

- $\alpha(\delta v(2u^{q+1}+v^{q+1})+\gamma u(u^{q+1}+2v^{q+1})+3(\theta u^2 v^q - u^q v^2)) = 3(uv(\gamma u + \delta v) + \theta u^3 - v^3)$
- $\delta u^q(u^{q+1}+2v^{q+1})+\gamma v^q(2u^{q+1}+v^{q+1})+3(\theta u v^{2q} - u^{2q} v) = 0$
- $uv(\delta^q u + \gamma^q v) + \theta^q v^3 - u^3 \neq 0$

Equivalence between $P_{0,\alpha}$ and $P_{\delta,1}$

A polynomial of the form $P_{0,\alpha}$ is equivalent to some $P_{\delta,1}$ if and only if the following hold for some $u, v \in \mathbb{F}_{q^2}$ with $u^{q+1} \neq v^{q+1}$:

- $3((v^3 - 3u^2v - u^3) + \alpha(u^{q+2} - u^q v^2 + u^2 v^q + 2uv^{q+1})) = \delta(3uv(u+v) - \alpha(u^{q+2} + 2uv(u+v)^q + v^{q+2}))$
- $3(u^{2q}v - 2u^{q+1}v^q - uv^{2q} - v^{2q+1}) = \delta(u^{2q+1} + 2(uv)^q(u+v) + v^{2q+1})$
- $u^3 - 3uv^2 - v^3 \neq \delta^q uv(u+v)$

A coding theory connection

Let $\mathcal{P}_q(n)$ be the set of all subspaces of $\mathbb{F}_q^n$. A subset $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is a *subspace code*, with distance between subspaces U and V given by

$$d(U, V) = \dim(U) + \dim(V) - 2\dim(U \cap V).$$

A coding theory connection

Let $\mathcal{P}_q(n)$ be the set of all subspaces of $\mathbb{F}_q^n$. A subset $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is a *subspace code*, with distance between subspaces U and V given by

$$d(U, V) = \mathrm{dim}(U) + \mathrm{dim}(V) - 2\mathrm{dim}(U \cap V).$$

Let G be a group acting on a metric set X and let $x \in X$. Then $xG = \{xg : g \in G\}$ is an *orbit code*. If G is cyclic, then xG is a *cyclic orbit code*.

A coding theory connection

$S_P = \ell_b C$ is a

- subspace code;
- cyclic orbit code;
- constant-dimension code;
- spread code.