Intersection Distribution and Its Application

Shuxing Li

Simon Fraser University

Joint work with Gohar Kyureghyan and Alexander Pott

Supported by PIMS Postdoctoral Fellowship

Carleton Finite Fields eSeminar

August 26 2020

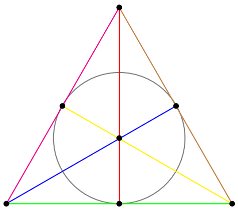
intersection distribution

$f \in \mathbb{F}_q[x]$
the collective
behaviour of
$\{f(x) + cx \mid c \in \mathbb{F}_q\}$

$(q+1)$-set S_f in
projective plane of order q
how S_f interacts with
lines in the plane

Outline

- Point sets in projective planes and polynomials over finite fields
- Oval polynomials and intersection distributions
- Intersection distribution of degree three polynomials
- Monomials with the same intersection distribution as x^3
- Application to Steiner triple systems



Fano plane: $7 = 2^2 + 2 + 1$ points and $7 = 2^2 + 2 + 1$ lines.

(1) Every line has $3 = 2 + 1$ points.

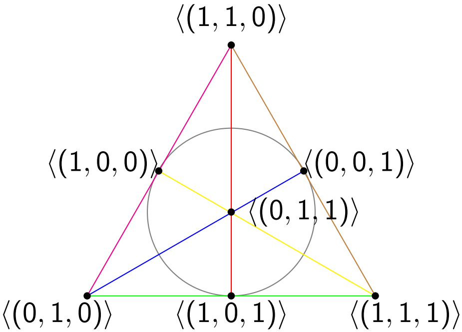
(2) Every two points are on one unique line.

(3) Every two lines intersect in exactly one point.

Projective plane of order 2: PP(2).

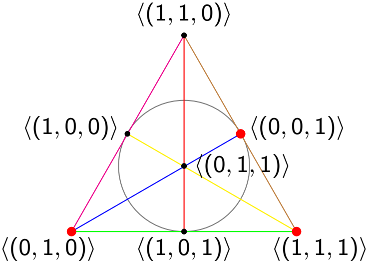
$2 \rightarrow$ prime power q: projective plane of order q, PP(q).

When q is a prime power, PP(q) can be derived from finite field $\mathbb{F}_q$.



affine part: $(*, *, 1)$. Exactly $\mathbb{F}_2^2$ in the above.
line at the infinity: $(*, *, 0)$.

$(q+1)$-set in $\mathrm{PP}(q)$ which has nice combinatorial characterization.



Characterization of an oval:
a $(q+1)$-set meeting all lines of $\mathrm{PP}(q)$ in either 0 or 1 or 2 points.

$$S_f = \underbrace{\{\langle(x, f(x), 1)\rangle \mid x \in \mathbb{F}_2\}}_{\text{affine part}} \cup \underbrace{\{\langle(0,1,0)\rangle\}}_{\text{on infinite line}}, \text{ where } f(x) = x^2.$$

A canonical $(q+1)$-set derived from $f \in \mathbb{F}_q[x]$:

$$S_f = \underbrace{\{\langle(x, f(x), 1)\rangle \mid x \in \mathbb{F}_q\}}_{\text{affine part}} \cup \underbrace{\{\langle(0,1,0)\rangle\}}_{\text{on infinite line}},$$

Remark

Under a mild assumption, every $(q+1)$-set in $PP(q)$ can be described as S_f for some polynomial f.

nice polynomials over $\mathbb{F}_q$ $\longleftrightarrow$ nice $(q+1)$-set in $\mathrm{PP}(q)$

Outline

- Point sets in projective planes and polynomials over finite fields
- Oval polynomials and intersection distributions
- Intersection distribution of degree three polynomials
- Monomials with the same intersection distribution as x^3
- Application to Steiner triple systems

An oval is a $(q+1)$-set meeting all lines of $\mathrm{PP}(q)$ in either 0 or 1 or 2 points.

Question

For which polynomial $f \in \mathbb{F}_q[x]$, the set

$$S_f = \{\langle (x, f(x), 1)\rangle \mid x \in \mathbb{F}_q\} \cup \{\langle (0,1,0)\rangle\}$$

is an oval?

An oval is a $(q+1)$-set meeting all lines of $\mathrm{PP}(q)$ in either 0 or 1 or 2 points.

Recall that S_f is an oval in $\mathrm{PP}(2)$ with $f(x) = x^2$. Note that $x^2 - bx - c = 0$ has at most two $\mathbb{F}_2$-solutions for each $(b, c) \in \mathbb{F}_2^2$.

Observation

$f \in \mathbb{F}_q[x]$ generates an oval S_f in $PP(q)$ if and only if for each $b \in \mathbb{F}_q$, the polynomial $f(x) - bx$ induces a mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$, so that every image has at most two preimages.

Hence, $f(x) = x^2$ is a canonical example.

Theorem (Segre (1955))

When q is odd, up to equivalence, S_f is an oval in $PP(q)$ if and only if $f(x) = x^2$.

q even: the situation is much more subtle since x^2 is $\mathbb{F}_2$-linear over $\mathbb{F}_q$.

Definition (o-polynomial)

Let q be an even prime power. A polynomial f is called an oval polynomial (o-polynomial) if S_f is an oval in $\mathrm{PP}(q)$.

Known o-monomials on $\mathbb{F}_{2^m}$

- x^{2^i}, $\gcd(i, m) = 1$
- x^6, m odd
- $x^{2^{2k}+2^k}$, $m = 4k - 1$
- $x^{2^{3k+1}+2^{2k+1}}$, $m = 4k + 1$
- $x^{3\cdot 2^k+4}$, $m = 2k - 1$ (for each $(b, c) \in \mathbb{F}_{2^m}^2$, $x^{3\cdot 2^k+4} - bx - c = 0$ has at most two $\mathbb{F}_{2^m}$-solutions)

Remark

An o-polynomial behaves like x^2 over $\mathbb{F}_{2^m}$ (x^2-like polynomial).

Not just ovals, o-polynomials can be used to construct cyclic difference sets, bent functions, linear codes, etc.

Observation

f is an o-polynomial if and only if

- *f is a permutation polynomial,*
- *$f(x) - bx$ is 2-to-1 for each $b \in \mathbb{F}_{2^m}^*$.*

f is an o-polynomial if and only if f is a permutation polynomial and $f(x) - bx$ is 2-to-1 for each $b \in \mathbb{F}_{2^m}^*$.

Example (Intersection distribution)

f o-polynomial over $\mathbb{F}_q = \mathbb{F}_{2^m}$. Count multiplicities in the following q multisets:

$\{\{f(x) \mid x \in \mathbb{F}_q\}\} \to \{\{1 \ (q \text{ times})\}\}$ (permutation)

for each $b \in \mathbb{F}_q^*$, $\{\{f(x) - bx \mid x \in \mathbb{F}_q\}\} \to \{\{0 \ (\frac{q}{2} \text{ times}), 2 \ (\frac{q}{2} \text{ times})\}\}$ (2-to-1)

the intersection distribution of f: $v_0(f) = \frac{q(q-1)}{2}$, $v_1(f) = q$, $v_2(f) = \frac{q(q-1)}{2}$.

f is an o-polynomial

$\longrightarrow$

$\longleftarrow$

f satisfying

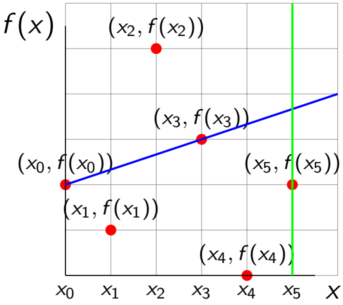
$$v_0(f) = \frac{q(q-1)}{2}$$
$$v_1(f) = q$$
$$v_2(f) = \frac{q(q-1)}{2}$$

Definition (Intersection distribution)

For $0 \leq i \leq q$, define

$$v_i(f) = |\{(b,c) \in \mathbb{F}_q^2 \mid f(x) - bx - c = 0 \text{ has exactly } i \text{ solutions in } \mathbb{F}_q\}|.$$

The sequence $(v_i(f))_{i=0}^{q}$ is the intersection distribution of f.



Geometric interpretation

The graph of f: $\{(x, f(x)) \mid x \in \mathbb{F}_q\}$.

$v_i(f)$: number of non-vertical lines intersect the graph of f in exactly i points.

Proposition (Li and Pott (2020))

$\{v_i(f) \mid 0 \leq i \leq q\} \leftrightarrow \{u_i(S_f) \mid 0 \leq i \leq q+1\}$.

f polynomial over $\mathbb{F}_q$ with $v_0(f) = \frac{q(q-1)}{2}$, $v_1(f) = q$, $v_2(f) = \frac{q(q-1)}{2}$, $v_i(f) = 0$ for $3 \leq i \leq q$.

$$\Downarrow$$

$\{u_i(S_f) \mid 0 \leq i \leq q+1\}$ known and S_f is an oval

$$\Downarrow$$

f is an o-polynomial

S_f line — S_f oval

$f(x) = ax + b$

$v_0(f) = q - 1$

minimum $v_0(f)$

?

$f(x) = x^2$ (q odd)

f o-polynomial (q even)

$v_0(f) = \frac{q(q-1)}{2}$

maximum $v_0(f)$

classification of o-monomials

To our best knowledge, very little is known about the collective behaviour of $\{x^d + cx \mid c \in \mathbb{F}_q\}$.

Outline

- Point sets in projective planes and polynomials over finite fields
- Oval polynomials and intersection distributions
- Intersection distribution of degree three polynomials
- Monomials with the same intersection distribution as x^3
- Application to Steiner triple systems

Theorem (Kyureghyan, Li, and Pott (2020+))

q a power of prime p. Let $f(x) = x^3 - ax^2$ be a polynomial over $\mathbb{F}_q$.

$p \neq 3$	$v_0(f) = \frac{q^2-1}{3}$, $v_1(f) = \frac{q^2-q+2}{2}$, $v_2(f) = q-1$, $v_3(f) = \frac{q^2-3q+2}{6}$
$p = 3$ $a = 0$	$v_0(f) = \frac{q(q-1)}{3}$, $v_1(f) = \frac{q(q+1)}{2}$, $v_2(f) = 0$, $v_3(f) = \frac{q(q-1)}{6}$
$p = 3$ $a \neq 0$	$v_0(f) = \frac{q^2}{3}$, $v_1(f) = \frac{q(q-1)}{2}$, $v_2(f) = q$, $v_3(f) = \frac{q(q-3)}{6}$

Corollary

Let q be a power of prime $p \neq 3$ and f arbitrary degree three polynomial over $\mathbb{F}_q$. We know the number of lines in $PP(q)$ intersecting S_f in 0, 1, 2 and 3 points.

One ingredient in the proof

Criterion determining the number of $\mathbb{F}_{3^m}$-solutions of $x^3 - x^2 - c = 0$, $c \in \mathbb{F}_{3^m}$.

Result

For $c \in \mathbb{F}_{3^m}$, suppose x_0 is a solution of $x^3 - x^2 - c = 0$.

$$|\{x \in \mathbb{F}_{3^m} \mid x^3 - x^2 - c = 0\}| = \begin{cases} 1 & 2x_0 + 1 \text{ is nonsquare,} \\ 2 & x_0 \in \{0, 1\}, \text{ or equivalently, } c = 0, \\ 3 & 2x_0 + 1 \text{ is nonzero square and } x_0 \neq 0. \end{cases}$$

Theorem (Kyureghyan, Li, and Pott (2020+))

q a power of prime p. Let $f(x) = x^3$ be a polynomial over $\mathbb{F}_q$.

$p \neq 3$	$v_0(f) = \frac{q^2-1}{3}$, $v_1(f) = \frac{q^2-q+2}{2}$, $v_2(f) = q-1$, $v_3(f) = \frac{q^2-3q+2}{6}$
$p = 3$	$v_0(f) = \frac{q(q-1)}{3}$, $v_1(f) = \frac{q(q+1)}{2}$, $v_2(f) = 0$, $v_3(f) = \frac{q(q-1)}{6}$

Characterize monomials with the same intersection distribution with x^3 (x^3-like monomials).

Recall that a x^2-like polynomial is just x^2 (q odd) or an o-polynomial (q even).

Outline

- Point sets in projective planes and polynomials over finite fields
- Oval polynomials and intersection distributions
- Intersection distribution of degree three polynomials
- Monomials with the same intersection distribution as x^3
- Application to Steiner triple systems

We derived a series of strong restrictions on x^3-like monomials (monomials with the same intersection distribution as x^3).

Theorem (Kyureghyan, Li, and Pott (2020+))

x^d over $\mathbb{F}_{3^m}$ is x^3-like if and only if the following holds:

(1) $\gcd(d-1, 3^m-1) = 2$,

(2) $\left.\frac{(x+1)^d-1}{x}\right|_{\mathbb{F}_{3^m}^*}$ *is 2-to-1.*

$$\frac{(x+1)^d-1}{x} = \frac{(x+1)^d-1^d}{x+1-1}$$

Conjecture (Kyureghyan, Li, and Pott (2020+))

The following is a complete list of x^3-like monomials x^d over $\mathbb{F}_q$ (plus the inverse if exists).

- *When $p = 2$,*
  - $d = 2^i + 1$, $\gcd(i, m) = 1$,
  - $d \equiv -2^i \pmod{q-1}$, $\gcd(i, m) = 1$, *m odd.*
- *When $p > 3$,*
  - $d = 3$,
- *When $p = 3$,*
  - $d = 3^i$, $\gcd(i, m) = 1$.
  - $d = 3^{(m+1)/2} + 2$, *m odd,*
  - $d = 2 \cdot 3^{m-1} + 1$, *m odd.*

For x^2-like polynomials: $p = 2$, o-polynomials, $p > 2$, x^2.

Two classes of conjectured x^3-like monomials x^d over $\mathbb{F}_{3^m}$:

- $d = 3^{(m+1)/2} + 2$, m odd,
- $d = 2 \cdot 3^{m-1} + 1$, m odd.

These exponents d also give m-sequences with 3-valued cross-correlation distribution. Cross-correlation distribution concerns the count of multiplicities in the multiset:

$$\{\{\mathrm{Tr}_{3^m/3}(x^d - bx) \mid x \in \mathbb{F}_{3^m}\}\}, \quad \text{for each } b \in \mathbb{F}_{3^m}.$$

In contrast, intersection distribution concerns the count of multiplicities in the multiset:

$$\{\{x^d - bx \mid x \in \mathbb{F}_{3^m}\}\}, \quad \text{for each } b \in \mathbb{F}_{3^m}.$$

S_f line

$f(x) = ax + b$

$v_0(f) = q - 1$

minimum $v_0(f)$

$f(x) = x^3$

$v_0(f) = \frac{q^2-1}{3}$, $(3, q) = 1$

$v_0(f) = \frac{q(q-1)}{3}$, $(3, q) = 3$

classification of
x^3-like monomials

S_f oval

$f(x) = x^2$ (q odd)

f o-polynomial (q even)

$v_0(f) = \frac{q(q-1)}{2}$

maximum $v_0(f)$

classification of o-monomials

S_f line — S_f oval

$f(x) = ax + b$	$f(x) = x^3$	$f(x) = x^2$ (q odd)
	$v_0(f) = \frac{q^2-1}{3}$, $(3,q) = 1$	f o-polynomial (q even)
$v_0(f) = q - 1$	$v_0(f) = \frac{q(q-1)}{3}$, $(3,q) = 3$	$v_0(f) = \frac{q(q-1)}{2}$
minimum $v_0(f)$		maximum $v_0(f)$

The intersection distribution of monomials x^d over $\mathbb{F}_q$ with $q = p^s$, where $d \in \{p^i, p^i + 1, \frac{q+1}{3}, \frac{q-1}{2}, \frac{q+1}{2}, \frac{2q}{3}, q-3, q-2, q-1\}$, $0 \le i \le s-1$, are determined.

An application: constructions of Kakeya sets in affine planes with prescribed sizes follow from the intersection distribution.

Two classes of conjectured x^3-like monomials x^d over $\mathbb{F}_{3^m}$:

- $d = 3^{(m+1)/2} + 2,\ m$ odd,
- $d = 2 \cdot 3^{m-1} + 1,\ m$ odd.

Outline

- Point sets in projective planes and polynomials over finite fields
- Oval polynomials and intersection distributions
- Intersection distribution of degree three polynomials
- Monomials with the same intersection distribution as x^3
- Application to Steiner triple systems

Steiner triple systems are one of the most well studied combinatorial configurations.

There are not many direct constructions of Steiner triples systems.

x^3 over $\mathbb{F}_{3^m}$, m odd

$\downarrow$

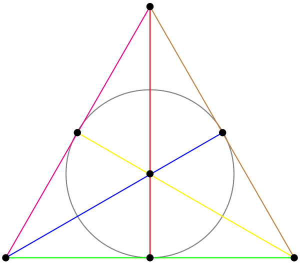
classical Steiner triple systems

$x^{3^{(m+1)/2}+2}$ over $\mathbb{F}_{3^m}$, m odd

$x^{2\cdot 3^{m-1}+1}$ over $\mathbb{F}_{3^m}$, m odd

$\downarrow$

new Steiner triple systems



Example (Steiner triple system)

point set: 7 points in PP(2)
block set: 7 lines in PP(2)
relation: 1. every block contains 3 points
2. every two distinct points uniquely determines a block

Example (affine triple system)

Let $\mathcal{V} = \mathbb{F}_{3^m}$ and

$$\mathcal{B} = \{\{x_1, x_2, x_3\} \mid x_1, x_2, x_3 \in \mathbb{F}_{3^m} \text{ distinct}, \ x_1 + x_2 + x_3 = 0\}.$$

Then $(\mathcal{V}, \mathcal{B})$ forms an Steiner triple system, named *affine triple system*.

For x^3 over $\mathbb{F}_q = \mathbb{F}_{3^m}$, we have

$$v_0(x^3) = \frac{q(q-1)}{3}, v_1(x^3) = \frac{q(q+1)}{2}, v_2(x^3) = 0, v_3(x^3) = \frac{q(q-1)}{6}.$$

Theorem (Kyureghyan, Li, and Pott (2020+))

Let f be a x^3-like polynomial over $\mathbb{F}_{3^m}$. Let $\mathcal{V} = \mathbb{F}_{3^m}$ and

$$\mathcal{B}_f = \{\{x_1, x_2, x_3\} \mid x_1, x_2, x_3 \in \mathbb{F}_{3^m} \text{ distinct}, \tfrac{f(x_3)-f(x_1)}{x_3-x_1} = \tfrac{f(x_2)-f(x_1)}{x_2-x_1}\}.$$

Then $(\mathcal{V}, \mathcal{B}_f)$ is a Steiner triple system. Moreover, $(\mathcal{V}, \mathcal{B}_f)$ is an affine triple system if $f(x) = x^3$ (or more generally, if and only if f is $\mathbb{F}_3$-linear).

x^3 over $\mathbb{F}_{3^m}$, m odd

$\downarrow$

affine triple systems

only known direct
construction on 3^m point
for many many years

$x^{3^{(m+1)/2}+2}$ over $\mathbb{F}_{3^m}$, m odd
$x^{2\cdot 3^{m-1}+1}$ over $\mathbb{F}_{3^m}$, m odd

$\downarrow$

new Steiner
triple systems
when $m \in \{3, 5\}$

"golden" monomials
gives new examples!

Concluding remarks

Research problem

(1) Compute the intersection distribution for more monomials, especially those with few nonzero entries.

(2) Prove that $x^{3^{(m+1)/2}+2}$ and $x^{2\cdot 3^{m-1}+1}$ are x^3-like over $\mathbb{F}_{3^m}$, m odd.

(3) Prove that the conjectured list of x^3-like polynomials is complete.

(4) Apply the "golden monomials" to coding theory, design theory, etc.

Main References

(1) G. Kyureghyan, S. Li, A. Pott. On the intersection distribution of degree three polynomials and related topics, *arXiv:2003.10040*, Submitted.

(2) S. Li, A. Pott, Intersection distribution, non-hitting index and Kakeya sets in affine planes, *Finite Fields Appl.*, 2020.