Intersection Distribution and Its Application

Shuxing Li

Simon Fraser University

Supported by PIMS Postdoctoral Fellowship

Joint work with Gohar Kyureghyan and Alexander Pott

Combinatorial Designs and Codes

July-14-2021

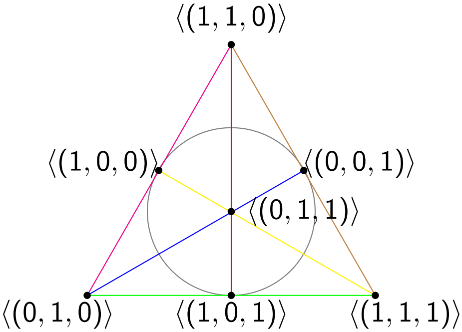
Steiner triple system

intersection distribution

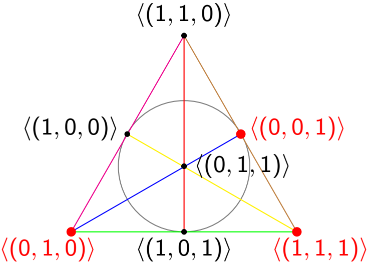
$f \in \mathbb{F}_q[x]$
the collective behaviour
of q polynomials
$\{f(x) + cx \mid c \in \mathbb{F}_q\}$

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

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



well-behaved $(q+1)$-set in $\mathrm{PP}(q)$



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

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

well-behaved $(q+1)$-sets in $\mathrm{PP}(q)$ $\longleftrightarrow$ well-behaved polynomials over $\mathbb{F}_q$

p prime, $q = p^m$, list of polynomials f over $\mathbb{F}_q$ such that S_f is an oval in $\mathrm{PP}(q)$.

- p odd, x^2

p prime, $q = p^m$, list of polynomials f over $\mathbb{F}_q$ such that S_f is an oval in $\mathrm{PP}(q)$.

- p odd, x^2
- $p = 2$, oval-polynomial (o-polynomial)
  1. x^{2^i}, $\gcd(i, m) = 1$
  2. x^6, m odd
  3. $x^{2^{2k}+2^k}$, $m = 4k - 1$
  4. $x^{2^{3k+1}+2^{2k+1}}$, $m = 4k + 1$
  5. $x^{3 \cdot 2^k + 4}$, $m = 2k - 1$
  6. $\dots$

p prime, $q = p^m$, list of polynomials f over $\mathbb{F}_q$ such that S_f is an oval in $\mathrm{PP}(q)$.

- p odd, x^2
- $p = 2$, oval-polynomial (o-polynomial)
  1. x^{2^i}, $\gcd(i, m) = 1$
  2. x^6, m odd
  3. $x^{2^{2k}+2^k}$, $m = 4k - 1$
  4. $x^{2^{3k+1}+2^{2k+1}}$, $m = 4k + 1$
  5. $x^{3\cdot 2^k+4}$, $m = 2k - 1$
  6. $\ldots$

Observation

$f \in \mathbb{F}_{2^m}[x]$ is an o-polynomial if and only if

(1) *f is a permutation polynomial,*

(2) *$f(x) - bx$ 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)

x^2 is o-polynomial over $\mathbb{F}_4$, where $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$.

$\{x^2 \mid x \in \mathbb{F}_4\} = \{0, 1, \alpha, \alpha^2\} \xrightarrow{\text{multiplicities}} \{1 \text{ (4 times)}\}$

$\{x^2 - x \mid x \in \mathbb{F}_4\} = \{0, 0, 1, 1\} \xrightarrow{\text{multiplicities}} \{0 \text{ (2 times)}, 2 \text{ (2 times)}\}$

$\{x^2 - \alpha x \mid x \in \mathbb{F}_4\} = \{0, 0, \alpha^2, \alpha^2\} \xrightarrow{\text{multiplicities}} \{0 \text{ (2 times)}, 2 \text{ (2 times)}\}$

$\{x^2 - \alpha^2 x \mid x \in \mathbb{F}_4\} = \{0, 0, \alpha, \alpha\} \xrightarrow{\text{multiplicities}} \{0 \text{ (2 times)}, 2 \text{ (2 times)}\}$

the intersection distribution of x^2: $v_0(x^2) = 6$, $v_1(x^2) = 4$, $v_2(x^2) = 6$.

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

---

f is an o-polynomial $\longrightarrow$ / $\longleftarrow$

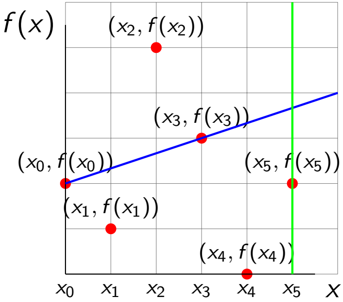
f satisfying

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

Definition (Intersection distribution)

The intersection distribution of $f \in \mathbb{F}_q[x]$ is a sequence $(v_i(f))_{i=0}^{q}$, where

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



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))

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

$\{v_i(f) \mid 0 \le i \le q\}$

$\{u_i(S_f) \mid 0 \le i \le q\}$
$u_i(S_f)$: number of lines in $\mathrm{PP}(q)$ intersecting S_f at exactly i points

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

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

characterization of o-polynomial	$\iff$	characterization of x^2-like polynomial (polynomial with the same intersection distribution as x^2)

The next simplest case: characterization of x^3-like monomial.

Theorem (Kyureghyan, Li, and Pott (2021))

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

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

Corollary

Let q be a prime power 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.

Theorem (Kyureghyan, Li, and Pott (2021))

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

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

Some necessary conditions of x^3-like monomials have been derived.

Conjecture (Kyureghyan, Li, and Pott (2021))

Up to taking the inverse, all x^3-like monomials over $\mathbb{F}_q = \mathbb{F}_{p^m}$:

- *When $p = 2$,*
  - ◇ $d = 2^i + 1$, $\gcd(i, m) = 1$,
  - ◇ $d \equiv -2^i \pmod{2^m - 1}$, $\gcd(i, m) = 1$, *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 (confirmed up to $m = 13$),*
  - ◇ $d = 2 \cdot 3^{m-1} + 1$, *m odd (confirmed up to $m = 13$).*

For x^2-like monomials: 1) $p = 2$, o-monomials, 2) $p > 2$, x^2.

Theorem (Li, Li, and Qu (preprint))

The two conjectured families of x^3-like monomials x^d over $\mathbb{F}_{3^m}$ have been confirmed:

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

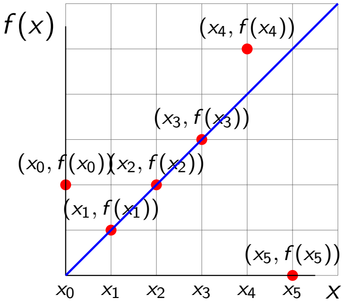
These two families are analogies of the o-polynomials in characteristic 3.

Steiner triple system form x^3-like polynomials

f is a x^3-like polynomial over $\mathbb{F}_{3^m}$

point set: $\mathbb{F}_{3^m}$

block set: $\{x_1, x_2, x_3\}$ is a block $\Leftrightarrow$ $(x_1, f(x_1))$, $(x_2, f(x_2))$, $(x_3, f(x_3))$ three collinear points on the graph $\{(x, f(x)) \mid x \in \mathbb{F}_{3^m}\}$.



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

classical Steiner triple systems over 3^m points

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

Steiner triple systems over 3^m points for each odd $m \geq 3$

new when $m \in \{3, 5\}$

Main References

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

(2) G. Kyureghyan, S. Li, A. Pott. On the intersection distribution of degree three polynomials and related topics, *Electronic Journal of Combinatorics*, 2021.

(3) Y. Li, K. Li, L. Qu. On two conjectures about the intersection distribution, *arXiv:2010.00312*.