The classification of planar monomials over fields of order a prime cubed

Irene Villa

University of Trento (Italy)

Seminario UMI Crittografia e Codici - De Cifris: MathCifris
-
02/02/2022

joint work with

Emily Bergman and Robert Coulter

University of Delaware (Newark - USA)

Preliminaries

We consider

- q a power of some odd prime p, $q = p^e$
- $\mathbb{F}_q$ finite field of q elements;
- $\mathbb{F}_q[x]$ ring of polynomials in x over $\mathbb{F}_q$: $f(x) = \sum_i a_i x^i$, with $a_i \in \mathbb{F}_q$
- $x^q - x$ field equation
- $f(x) = \sum_{i=0}^{q-1} a_i x^i$, $a_i \in \mathbb{F}_q$

Preliminaries

We consider

- q a power of some odd prime p, $q = p^e$
- $\mathbb{F}_q$ finite field of q elements;
- $\mathbb{F}_q[x]$ ring of polynomials in x over $\mathbb{F}_q$: $f(x) = \sum_i a_i x^i$, with $a_i \in \mathbb{F}_q$
- $x^q - x$ field equation
- $f(x) = \sum_{i=0}^{q-1} a_i x^i$, $a_i \in \mathbb{F}_q$

Definition

A polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) if it induces a bijection of $\mathbb{F}_q$ under the evaluation map $y \to f(y)$.

Preliminaries

We consider

- q a power of some odd prime p, $q = p^e$
- $\mathbb{F}_q$ finite field of q elements;
- $\mathbb{F}_q[x]$ ring of polynomials in x over $\mathbb{F}_q$: $f(x) = \sum_i a_i x^i$, with $a_i \in \mathbb{F}_q$
- $x^q - x$ field equation
- $f(x) = \sum_{i=0}^{q-1} a_i x^i$, $a_i \in \mathbb{F}_q$

Definition

A polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) if it induces a bijection of $\mathbb{F}_q$ under the evaluation map $y \to f(y)$.

DO polynomial (Dembowski-Ostrom)

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

Planar functions

Definition

A polynomial $f \in \mathbb{F}_q[x]$ is called planar if for every nonzero $a \in \mathbb{F}_q$, the polynomial $f(x+a) - f(x)$ is a PP over $\mathbb{F}_q$.

Planar functions

- Planar functions were introduced by Dembowski and Ostrom in 1968 in the context of finite geometry to describe projective planes with specific properties.

Planar functions

- Planar functions were introduced by Dembowski and Ostrom in 1968 in the context of finite geometry to describe projective planes with specific properties.
- Planar DO polynomials are in 1-to-1 correspondence with commutative presemifields of odd order $\mathbb{S} = (\mathbb{F}_q, +, \star)$:

Planar functions

- Planar functions were introduced by Dembowski and Ostrom in 1968 in the context of finite geometry to describe projective planes with specific properties.
- Planar DO polynomials are in 1-to-1 correspondence with commutative presemifields of odd order $\mathbb{S} = (\mathbb{F}_q, +, \star)$:
  - $f \Rightarrow x \star y := f(x+y) - f(x) - f(y)$,

Planar functions

- Planar functions were introduced by Dembowski and Ostrom in 1968 in the context of finite geometry to describe projective planes with specific properties.
- Planar DO polynomials are in 1-to-1 correspondence with commutative presemifields of odd order $\mathbb{S} = (\mathbb{F}_q, +, \star)$:
  - $f \Rightarrow x \star y := f(x+y) - f(x) - f(y)$,
  - $\mathbb{S} \Rightarrow f(x) := \frac{1}{2}(x \star x)$.

Planar functions

- Planar functions were introduced by Dembowski and Ostrom in 1968 in the context of finite geometry to describe projective planes with specific properties.
- Planar DO polynomials are in 1-to-1 correspondence with commutative presemifields of odd order $\mathbb{S} = (\mathbb{F}_q, +, \star)$:
  - $f \Rightarrow x \star y := f(x+y) - f(x) - f(y)$,
  - $\mathbb{S} \Rightarrow f(x) := \frac{1}{2}(x \star x)$.
- Planar functions correspond to *perfect nonlinear* maps ($\delta_f = 1$)

$$\delta_f = \max_{a,b \in \mathbb{F}_q, a \neq 0} |\{x \in \mathbb{F}_q \ : \ f(x+a) - f(x) = b\}|.$$

Planar functions

- Planar functions were introduced by Dembowski and Ostrom in 1968 in the context of finite geometry to describe projective planes with specific properties.
- Planar DO polynomials are in 1-to-1 correspondence with commutative presemifields of odd order $\mathbb{S} = (\mathbb{F}_q, +, \star)$:
  - $f \Rightarrow x \star y := f(x+y) - f(x) - f(y)$,
  - $\mathbb{S} \Rightarrow f(x) := \frac{1}{2}(x \star x)$.
- Planar functions correspond to *perfect nonlinear* maps ($\delta_f = 1$)

$$\delta_f = \max_{a,b \in \mathbb{F}_q, a \neq 0} |\{x \in \mathbb{F}_q \ : \ f(x+a) - f(x) = b\}|.$$

$\rightarrow$ Planar functions exist only for p odd (*almost perfect nonlinear* if $\delta_f = 2$).

Planar functions

- Planar functions were introduced by Dembowski and Ostrom in 1968 in the context of finite geometry to describe projective planes with specific properties.
- Planar DO polynomials are in 1-to-1 correspondence with commutative presemifields of odd order $\mathbb{S} = (\mathbb{F}_q, +, \star)$:
  - $f \Rightarrow x \star y := f(x+y) - f(x) - f(y)$,
  - $\mathbb{S} \Rightarrow f(x) := \frac{1}{2}(x \star x)$.
- Planar functions correspond to *perfect nonlinear* maps ($\delta_f = 1$)

$$\delta_f = \max_{a,b \in \mathbb{F}_q, a \neq 0} |\{x \in \mathbb{F}_q \ : \ f(x+a) - f(x) = b\}|.$$

→ Planar functions exist only for p odd (*almost perfect nonlinear* if $\delta_f = 2$).

→ Planar functions cannot be PP.

The Dembowski-Ostrom Conjecture (1968)

Ignoring contants and linear terms, the only planar functions over finite fields are DO polynomials.

The Dembowski-Ostrom Conjecture (1968)

Ignoring contants and linear terms, the only planar functions over finite fields are DO polynomials.

- Over $\mathbb{F}_p$ the conjecture is true (in 1987 Johnson for the monomial case; independently by Gluck 1990, Hiramine 1989 and Rónyai and Szönyi 1989).

The Dembowski-Ostrom Conjecture (1968)

Ignoring contants and linear terms, the only planar functions over finite fields are DO polynomials.

- Over $\mathbb{F}_p$ the conjecture is true (in 1987 Johnson for the monomial case; independently by Gluck 1990, Hiramine 1989 and Rónyai and Szönyi 1989).
- Over $\mathbb{F}_{3^n}$ the conjecture is false (x^{14} over $\mathbb{F}_{3^4}$) (Coulter and Matthews 1997: $x^{\frac{3^t+1}{2}}$ over $\mathbb{F}_{3^n}$ with t odd and $\gcd(t, n) = 1$).

The Dembowski-Ostrom Conjecture (1968)

Ignoring contants and linear terms, the only planar functions over finite fields are DO polynomials.

- Over $\mathbb{F}_p$ the conjecture is true (in 1987 Johnson for the monomial case; independently by Gluck 1990, Hiramine 1989 and Rónyai and Szönyi 1989).
- Over $\mathbb{F}_{3^n}$ the conjecture is false (x^{14} over $\mathbb{F}_{3^4}$) (Coulter and Matthews 1997: $x^{\frac{3^t+1}{2}}$ over $\mathbb{F}_{3^n}$ with t odd and $\gcd(t,n)=1$).
- Over $\mathbb{F}_{p^2}$ true for monomials (Coulter 2006).

The Dembowski-Ostrom Conjecture (1968)

Ignoring contants and linear terms, the only planar functions over finite fields are DO polynomials.

- Over $\mathbb{F}_p$ the conjecture is true (in 1987 Johnson for the monomial case; independently by Gluck 1990, Hiramine 1989 and Rónyai and Szönyi 1989).
- Over $\mathbb{F}_{3^n}$ the conjecture is false (x^{14} over $\mathbb{F}_{3^4}$) (Coulter and Matthews 1997: $x^{\frac{3^t+1}{2}}$ over $\mathbb{F}_{3^n}$ with t odd and $\gcd(t,n)=1$).
- Over $\mathbb{F}_{p^2}$ true for monomials (Coulter 2006).
- Over $\mathbb{F}_{p^4}$ true for monomials with $p \geq 5$ (Coulter and Lazebnik 2012).

The Dembowski-Ostrom Conjecture (1968)

Ignoring contants and linear terms, the only planar functions over finite fields are DO polynomials.

- Over $\mathbb{F}_p$ the conjecture is true (in 1987 Johnson for the monomial case; independently by Gluck 1990, Hiramine 1989 and Rónyai and Szönyi 1989).
- Over $\mathbb{F}_{3^n}$ the conjecture is false (x^{14} over $\mathbb{F}_{3^4}$) (Coulter and Matthews 1997: $x^{\frac{3^t+1}{2}}$ over $\mathbb{F}_{3^n}$ with t odd and $\gcd(t,n)=1$).
- Over $\mathbb{F}_{p^2}$ true for monomials (Coulter 2006).
- Over $\mathbb{F}_{p^4}$ true for monomials with $p \geq 5$ (Coulter and Lazebnik 2012).
- Over $\mathbb{F}_{p^n}$ with $p \geq 5$ the conjecture remains open.

The prime field classification of planar monomials gives a small impact on the classification of any finite field.

If x^n is planar over $\mathbb{F}_{p^e}$ then $n \equiv 2 \bmod (p-1)$.

The prime field classification of planar monomials gives a small impact on the classification of any finite field.

If x^n is planar over $\mathbb{F}_{p^e}$ then $n \equiv 2 \bmod (p-1)$.

Apart from this, we have no additional info on the case $q = p^3$.

The prime field classification of planar monomials gives a small impact on the classification of any finite field.

If x^n is planar over $\mathbb{F}_{p^e}$ then $n \equiv 2 \bmod (p-1)$.

Apart from this, we have no additional info on the case $q = p^3$.

Question

What about monomials over $\mathbb{F}_{p^3}$?

Planar monomials

The condition of planarity simplifies significantly in the monomial case.

- x^n is planar over $\mathbb{F}_q$ if and only if the polynomial $(x+1)^n - x^n$ is a PP.
- If x^n is planar then $n \equiv 2 \mod (p-1)$ and $\gcd(n, q-1) = 2$.

Planar monomials

The condition of planarity simplifies significantly in the monomial case.

- x^n is planar over $\mathbb{F}_q$ if and only if the polynomial $(x+1)^n - x^n$ is a PP.
- If x^n is planar then $n \equiv 2 \mod (p-1)$ and $\gcd(n, q-1) = 2$.

$$\boxed{f_n(x) = (x+1)^n - x^n} \text{ and } \boxed{n \leq q-3}$$

Lemma (Hermite's criteria)

A polynomial $f \in \mathbb{F}_q[x]$, is a PP over $\mathbb{F}_q$ if and only if

(i) *f has exactly one root in $\mathbb{F}_q$, and*

(ii) *the reduction $f^t \bmod (x^q - x)$, with $0 < t < q - 1$ and $t \not\equiv 0 \bmod p$, has degree less than $q - 1$.*

Lemma (Hermite's criteria)

A polynomial $f \in \mathbb{F}_q[x]$, is a PP over $\mathbb{F}_q$ if and only if

(i) *f has exactly one root in $\mathbb{F}_q$, and*

(ii) *the reduction $f^t \bmod (x^q - x)$, with $0 < t < q-1$ and $t \not\equiv 0 \bmod p$, has degree less than $q-1$.*

If we find an Hermite exponent $0 < t < q-1$ such that $f_n^t \bmod (x^q - x)$ has degree $q-1$, then x^n is not planar over $\mathbb{F}_q$.

base-p expansion

For $a < q = p^e$, the base-p exapansion of a is $(a_{e-1} \cdots a_0)_p$, where $0 \leq a_i < p$ are such that $a = a_0 + a_1 p + \cdots + a_{e-1} p^{e-1}$.

1. x^n is planar if and only if x^{np} is planar.

2. If x^n is planar over $\mathbb{F}_q$, then it is planar over $\mathbb{F}_p$.

1. x^n is planar if and only if x^{np} is planar.

$$n = (a_{e-1} \cdots a_0)_p \text{ and } np = (a_{e-2} \cdots a_0 a_{e-1})_p,$$

so we may cycle the base-p digits of n around and place the largest a_i in the most significant bit.

2. If x^n is planar over $\mathbb{F}_q$, then it is planar over $\mathbb{F}_p$.

1. x^n is planar if and only if x^{np} is planar.

$$n = (a_{e-1} \cdots a_0)_p \text{ and } np = (a_{e-2} \cdots a_0 a_{e-1})_p,$$

so we may cycle the base-p digits of n around and place the largest a_i in the most significant bit.

2. If x^n is planar over $\mathbb{F}_q$, then it is planar over $\mathbb{F}_p$.

Hence $n \equiv 2 \mod (p-1)$, that is

$$S = a_0 + a_1 + \cdots + a_{e-1} \equiv 2 \bmod (p-1).$$

1. x^n is planar if and only if x^{np} is planar.

$$n = (a_{e-1} \cdots a_0)_p \text{ and } np = (a_{e-2} \cdots a_0 a_{e-1})_p,$$

so we may cycle the base-p digits of n around and place the largest a_i in the most significant bit.

2. If x^n is planar over $\mathbb{F}_q$, then it is planar over $\mathbb{F}_p$.

Hence $n \equiv 2 \mod (p-1)$, that is

$$S = a_0 + a_1 + \cdots + a_{e-1} \equiv 2 \bmod (p-1).$$

In our specific case, $q = p^3$ and $n = (a_2 a_1 a_0)_p$, we have

- Case 1. $S = 2$,
- Case 2. $S = 2p$,
- Case 3. $S = p + 1$.

Case 1: $S = 2$

- If $S = 2$ then $x^n = x^{p^i + p^j}$.
- Coulter and Matthews showed that $x^{p^i+p^j}$ is planar over $\mathbb{F}_{p^e}$ if and only if $e/\gcd(j-i, e)$ is odd.

Case 1: $S = 2$

- If $S = 2$ then $x^n = x^{p^i + p^j}$.
- Coulter and Matthews showed that $x^{p^i+p^j}$ is planar over $\mathbb{F}_{p^e}$ if and only if $e/\gcd(j-i, e)$ is odd.

Proposition

If $S = 2$, then $n = p^i + p^j$ with $0 \leq i \leq j < 3$, and x^n is always planar over $\mathbb{F}_{p^3}$.

Approach for other cases

1. $n = (a_2 a_1 a_0)_p$, $f_n(x) = (x+1)^n - x^n$
2. t Hermite exponent
3. if f_n^t has maximal degree then f_n is not PP
4. then x^n is not planar

Case 2 : $S = 2p$

Proposition

If $S = 2p$. then the Hermite exponent $t = p + 1$ shows that f_n is never a PP over $\mathbb{F}_{p^3}$. Hence, x^n is never planar over $\mathbb{F}_{p^3}$.

Case 3: $S = p + 1$

Proposition

Let $n = (a_2 a_1 a_0)_p$, $S = p + 1$, $a_2 \geq a_0, a_1$ and $a_i \geq 2$ for $i = 0, 1, 2$.

- *If $a_2 > (p+1)/2$, then the Hermite exponent $t = 2 + p + p^2$ shows that f_n is not a PP over $\mathbb{F}_{p^3}$.*
- *If $a_2 \leq (p+1)/2$, then it is impossible for the two Hermite exponents $t_1 = 2 + p + p^2$ and $t_2 = 2 + 2p$ to both fail to show f_n is not a PP over $\mathbb{F}_{p^3}$.*

Thus x^n is not planar over $\mathbb{F}_{p^3}$.

Case 3: $S = p + 1$

Proposition

Let $n = (a_2 a_1 a_0)_p$, $S = p + 1$, $a_2 \geq a_1, a_0$ and $a_i < 2$ for at least one $i \in \{0, 1\}$. The Hermite exponent $t = 2 + 2p + 2p^2$ shows f_n is not a PP over $\mathbb{F}_{p^3}$ for all but 11 specific choices of n.

Case 3: $S = p + 1$

Proposition

Let $n = (a_2 a_1 a_0)_p$, $S = p + 1$, $a_2 \geq a_1, a_0$ and $a_i < 2$ for at least one $i \in \{0, 1\}$. The Hermite exponent $t = 2 + 2p + 2p^2$ shows f_n is not a PP over $\mathbb{F}_{p^3}$ for all but 11 specific choices of n.

1. $n = \frac{p+1}{2}(p + p^2)$
2. $n = \frac{p+1}{2}(1 + p^2)$
3. $n = 1 + (\frac{p+1}{2} - 1)p + \frac{p+1}{2}p^2$
4. $n = (\frac{p+1}{2} - 1) + p + \frac{p+1}{2}p^2$
5. $n = (\frac{p+1}{2} - 1) + (\frac{p+1}{2} + 1)p^2$
6. $n = 1 + 3p + (p - 3)p^2$
7. $n = 1 + 2p + (p - 2)p^2$
8. $n = 2 + p + (p - 2)p^2$
9. $n = 2 + (p - 1)p^2$
10. $n = 2p + (p - 1)p^2$
11. $n = 1 + p + (p - 1)p^2$

Case 3: $S = p + 1$

Also for these 11 exceptions there exist Hermite exponents showing that f_n is not PP over $\mathbb{F}_{p^3}$.

1. with $t = (p-2) + p$ and $t = (p-6) + p + 4p^2$,
2. with $t = (p-2) + p$ and $t = (p-6) + p + 4p^2$,
3. with $t = 2p + 4p^2$,
4. with $t = (p-2) + p$,
5. with $t = (p-6) + p + 2p^2$,
6. with $t = 2 + 4p + 4p^2$,
7. with $t = (p-1)(p+12)$,
8. with $t = 1 + 2p + 3p^2$,
9. with $t = 1 + 2p + 3p^2$,
10. with $t = 2 + (p-1)p$,
11. with $t = p - 1$.

Case 3: $S = p + 1$

Proposition

If $S = p + 1$, then x^n is never planar over $\mathbb{F}_{p^3}$.

Classification of planar monomials over $\mathbb{F}_{p^3}$

Theorem

Let $q = p^3$ with p an odd prime. The monomial x^n is planar over $\mathbb{F}_q$ if and only if $n = p^i + p^j \mod (q-1)$ with $0 \leq i, j < 3$. That is, the Dembowski-Ostrom Conjecture is true over $\mathbb{F}_{p^3}$ for monomials.

How did we prove all that?

1. Extensive computations to find which Hermite exponents work for which "group" of exponents n (for at least all "small" p's).
2. Given t and n, try to prove "by hand" that f_n^t has maximal degree for a general odd prime p.

$$f_n(x) = (x+1)^n - x^n$$
$$f_n^t(x) = \sum_{i=0}^{t} \binom{t}{i} (-1)^{t-i} (x+1)^{ni} x^{n(t-i)}$$

$$f_n(x) = (x+1)^n - x^n$$

$$f_n^t(x) = \sum_{i=0}^{t} \binom{t}{i} (-1)^{t-i} (x+1)^{ni} x^{n(t-i)}$$

Lemma (Lucas)

Let p be a prime and $\alpha \geq \beta$ be positive integers with α and β having base-p expansions $\alpha = (\alpha_r \cdots \alpha_0)_p$ and $\beta = (\beta_r \ldots \beta_0)_p$ respectively. Then

$$\binom{\alpha}{\beta} \equiv \prod_{i=0}^{r} \binom{\alpha_i}{\beta_i} \bmod p,$$

where $\binom{n}{k} = 0$ if $n < k$.

How to check that $f_n(x) = (x+1)^n - x^n$ is not a PP

How to check that $f_n(x) = (x+1)^n - x^n$ is not a PP

1. Expansion

$$f_n^t(x) = \sum_{i=0}^{t} \binom{t}{i} (-1)^{t-i} (x+1)^{ni} x^{n(t-i)} = \sum_{(\alpha,\beta)} C_{(\alpha,\beta)} (x+1)^{n\alpha} x^{n\beta}$$

How to check that $f_n(x) = (x+1)^n - x^n$ is not a PP

1. Expansion

$$f_n^t(x) = \sum_{i=0}^{t} \binom{t}{i} (-1)^{t-i} (x+1)^{ni} x^{n(t-i)} = \sum_{(\alpha,\beta)} C_{(\alpha,\beta)} (x+1)^{n\alpha} x^{n\beta}$$

2. Reduction

$$n\alpha = r = (r_2 r_1 r_0)_p \text{ with } 0 \leq r_i \leq p-1$$
$$n\beta = s = (s_2 s_1 s_0)_p \text{ with } 0 \leq s_i \leq p-1$$

How to check that $f_n(x) = (x+1)^n - x^n$ is not a PP

1. Expansion

$$f_n^t(x) = \sum_{i=0}^{t} \binom{t}{i} (-1)^{t-i} (x+1)^{ni} x^{n(t-i)} = \sum_{(\alpha,\beta)} C_{(\alpha,\beta)} (x+1)^{n\alpha} x^{n\beta}$$

2. Reduction

$$n\alpha = r = (r_2 r_1 r_0)_p \text{ with } 0 \leq r_i \leq p-1$$
$$n\beta = s = (s_2 s_1 s_0)_p \text{ with } 0 \leq s_i \leq p-1$$

3. Multiplication

$$(x+1)^{(r_2 r_1 r_0)_p} x^{(s_2 s_1 s_0)_p} = \sum_{j_0=0}^{r_0} \sum_{j_1=0}^{r_1} \sum_{j_2=0}^{r_2} \binom{r_0}{j_0} \binom{r_1}{j_1} \binom{r_2}{j_2} x^{(j_2 j_1 j_0)_p} x^{(s_2 s_1 s_0)_p}$$

How to check that $f_n(x) = (x+1)^n - x^n$ is not a PP

1. Expansion

$$f_n^t(x) = \sum_{i=0}^{t} \binom{t}{i} (-1)^{t-i} (x+1)^{ni} x^{n(t-i)} = \sum_{(\alpha,\beta)} C_{(\alpha,\beta)} (x+1)^{n\alpha} x^{n\beta}$$

2. Reduction

$$n\alpha = r = (r_2 r_1 r_0)_p \text{ with } 0 \leq r_i \leq p-1$$
$$n\beta = s = (s_2 s_1 s_0)_p \text{ with } 0 \leq s_i \leq p-1$$

3. Multiplication

$$(x+1)^{(r_2 r_1 r_0)_p} x^{(s_2 s_1 s_0)_p} = \sum_{j_0=0}^{r_0} \sum_{j_1=0}^{r_1} \sum_{j_2=0}^{r_2} \binom{r_0}{j_0} \binom{r_1}{j_1} \binom{r_2}{j_2} x^{(j_2 j_1 j_0)_p} x^{(s_2 s_1 s_0)_p}$$

4. Coefficient

$$coeff = C_{(\alpha,\beta)} \binom{r_0}{j_0} \binom{r_1}{j_1} \binom{r_2}{j_2} \qquad \sum coeff \not\equiv 0 \bmod p$$

Some examples of cases studied

Example [No. 8]

$n = 2 + p + (p-2)p^2$ and $t = 1 + 2p + 3p^2$ (set $y = x + 1$)

$$\begin{aligned}
f_n^t(x) = \; & y^{2+p+9p^2} - 3y^{1+3p+6p^2}x^{1+(p-2)p+2p^2} + 3y^{5p+3p^2}x^{2+(p-4)p+5p^2} - y^{(p-1)+6p}x^{3+(p-6)p+8p^2} \\
& - 2y^{4+(p-2)p+7p^2}x^{(p-2)+2p+p^2} + 6y^{3+5p^2}x^{(p-1)+4p^2} - 6y^{2+2p+2p^2}x^{(p-1)p+6p^2} \\
& + 2y^{4p+(p-1)p^2}x^{1+(p-3)p+9p^2} + y^{6+(p-5)p+6p^2}x^{(p-4)+5p+2p^2} - 3y^{5+(p-3)p+3p^2}x^{(p-3)+3p+5p^2} \\
& + 3y^{4+(p-1)p}x^{(p-2)+p+8p^2} - y^{2+p+(p-2)p^2}x^{(p-1)+(p-1)p+10p^2} - y^{(p-1)+(p-1)p+10p^2}x^{2+p+(p-2)p^2} \\
& + 3y^{(p-2)+p+8p^2}x^{4+(p-1)p} - 3y^{(p-3)+3p+5p^2}x^{5+(p-3)p+3p^2} + y^{(p-4)+5p+2p^2}x^{6+(p-5)+6p^2} \\
& + 2y^{1+(p-3)p+9p^2}x^{4p+(p-1)p^2} - 6y^{5+(p-3)p+3p^2}x^{2+2p+2p^2} + 6y^{(p-1)+4p^2}x^{3+5p^2} \\
& - 2y^{(p-2)+2p+p^2}x^{4+(p-2)p+7p^2} - y^{3+(p-6)p+8p^2}x^{(p-1)+6p} + 3y^{2+(p-4)p+5p^2}x^{5p+3p^2} \\
& - 3y^{1+(p-2)p+2p^2}x^{1+3p+6p^2} + x^{2+p+9p^2}.
\end{aligned}$$

Example [No. 8]

$n = 2 + p + (p-2)p^2$ and $t = 1 + 2p + 3p^2$ (set $y = x + 1$)

$$
\begin{aligned}
f_n^t(x) = {} & y^{2+p+9p^2} - 3y^{1+3p+6p^2}x^{1+(p-2)p+2p^2} + 3y^{5p+3p^2}x^{2+(p-4)p+5p^2} - y^{(p-1)+6p}x^{3+(p-6)p+8p^2} \\
& - 2y^{4+(p-2)p+7p^2}x^{(p-2)+2p+p^2} + 6y^{3+5p^2}x^{(p-1)+4p^2} - 6y^{2+2p+2p^2}x^{(p-1)p+6p^2} \\
& + 2y^{4p+(p-1)p^2}x^{1+(p-3)p+9p^2} + y^{6+(p-5)p+6p^2}x^{(p-4)+5p+2p^2} - 3y^{5+(p-3)p+3p^2}x^{(p-3)+3p+5p^2} \\
& + 3y^{4+(p-1)p}x^{(p-2)+p+8p^2} - y^{2+p+(p-2)p^2}x^{(p-1)+(p-1)p+10p^2} - y^{(p-1)+(p-1)p+10p^2}x^{2+p+(p-2)p^2} \\
& + 3y^{(p-2)+p+8p^2}x^{4+(p-1)p} - 3y^{(p-3)+3p+5p^2}x^{5+(p-3)p+3p^2} + y^{(p-4)+5p+2p^2}x^{6+(p-5)+6p^2} \\
& + 2y^{1+(p-3)p+9p^2}x^{4p+(p-1)p^2} - 6y^{5+(p-3)p+3p^2}x^{2+2p+2p^2} + 6y^{(p-1)+4p^2}x^{3+5p^2} \\
& - 2y^{(p-2)+2p+p^2}x^{4+(p-2)p+7p^2} - y^{3+(p-6)p+8p^2}x^{(p-1)+6p} + 3y^{2+(p-4)p+5p^2}x^{5p+3p^2} \\
& - 3y^{1+(p-2)p+2p^2}x^{1+3p+6p^2} + x^{2+p+9p^2}.
\end{aligned}
$$

$$
y^{2+p+(p-2)p^2}x^{(p-1)+(p-1)p+10p^2} = \sum \binom{2}{\alpha_0}\binom{1}{\alpha_1}\binom{p-2}{\alpha_2} x^{(p-1+\alpha_0)+(p-1+\alpha_1)p+(10+\alpha_2)p^2}
$$

$$
y^{(p-1)+(p-1)p+10p^2}x^{2+p+(p-2)p^2} = \sum \binom{p-1}{\alpha_0}\binom{p-1}{\alpha_1}\binom{10}{\alpha_2} x^{(2+\alpha_0)+(1+\alpha_1)p+(p-2+\alpha_2)p^2}
$$

Example [No. 8]

$n = 2 + p + (p-2)p^2$ and $t = 1 + 2p + 3p^2$ (set $y = x+1$)

$$
\begin{aligned}
f_n^t(x) = \ & y^{2+p+9p^2} - 3y^{1+3p+6p^2}x^{1+(p-2)p+2p^2} + 3y^{5p+3p^2}x^{2+(p-4)p+5p^2} - y^{(p-1)+6p}x^{3+(p-6)p+8p^2} \\
& - 2y^{4+(p-2)p+7p^2}x^{(p-2)+2p+p^2} + 6y^{3+5p^2}x^{(p-1)+4p^2} - 6y^{2+2p+2p^2}x^{(p-1)p+6p^2} \\
& + 2y^{4p+(p-1)p^2}x^{1+(p-3)p+9p^2} + y^{6+(p-5)p+6p^2}x^{(p-4)+5p+2p^2} - 3y^{5+(p-3)p+3p^2}x^{(p-3)+3p+5p^2} \\
& + 3y^{4+(p-1)p}x^{(p-2)+p+8p^2} - y^{2+p+(p-2)p^2}x^{(p-1)+(p-1)p+10p^2} - y^{(p-1)+(p-1)p+10p^2}x^{2+p+(p-2)p^2} \\
& + 3y^{(p-2)+p+8p^2}x^{4+(p-1)p} - 3y^{(p-3)+3p+5p^2}x^{5+(p-3)p+3p^2} + y^{(p-4)+5p+2p^2}x^{6+(p-5)+6p^2} \\
& + 2y^{1+(p-3)p+9p^2}x^{4p+(p-1)p^2} - 6y^{5+(p-3)p+3p^2}x^{2+2p+2p^2} + 6y^{(p-1)+4p^2}x^{3+5p^2} \\
& - 2y^{(p-2)+2p+p^2}x^{4+(p-2)p+7p^2} - y^{3+(p-6)p+8p^2}x^{(p-1)+6p} + 3y^{2+(p-4)p+5p^2}x^{5p+3p^2} \\
& - 3y^{1+(p-2)p+2p^2}x^{1+3p+6p^2} + x^{2+p+9p^2}.
\end{aligned}
$$

$$y^{2+p+(p-2)p^2}x^{(p-1)+(p-1)p+10p^2} = \sum \binom{2}{\alpha_0}\binom{1}{\alpha_1}\binom{p-2}{\alpha_2}x^{(p-1+\alpha_0)+(p-1+\alpha_1)p+(10+\alpha_2)p^2}$$

$$y^{(p-1)+(p-1)p+10p^2}x^{2+p+(p-2)p^2} = \sum \binom{p-1}{\alpha_0}\binom{p-1}{\alpha_1}\binom{10}{\alpha_2}x^{(2+\alpha_0)+(1+\alpha_1)p+(p-2+\alpha_2)p^2}$$

$$\binom{2}{0}\binom{1}{0}\binom{p-2}{p-11} = -10, \qquad \binom{p-1}{p-3}\binom{p-1}{p-2}\binom{10}{1} = -10$$

A more complex example

$S = p+1$, $n = (a_2a_1a_0)_p$, $2 \le a_0, a_1 \le a_2$, $a_2 > (p+1)/2$ and $t = 2+p+p^2$

$$f_n^t(x) =$$

$$x^{(2+a_1)+(2+a_2)p+(2+a_0)p^2} + 2x^{2+2p+2p^2}y^{a_0+a_1p+a_2p^2} + x^{(a_2+a_1)+(a_0+a_2)p+(a_0+a_1)p^2}y^{2a_0+2a_1p+2a_2p^2}$$

$$+x^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2}y^{a_2+a_0p+a_1p^2} + 2x^{(a_0+a_1)+(a_1+a_2)p+(a_2+a_0)p^2}y^{(a_0+a_2)+(a_1+a_0)p+(a_2+a_1)p^2}$$

$$+x^{a_1+a_2p+a_0p^2}y^{(2a_0+a_2)+(2a_1+a_0)p+(2a_2+a_1)p^2} + y^{(2+a_1)+(2+a_2)p+(2+a_0)p^2} + 2x^{a_0+a_1p+a_2p^2}y^{2+2p+2p^2}$$

$$+x^{2a_0+2a_1p+2a_2p^2}y^{(a_1+a_2)+(a_0+a_2)p+(a_0+a_1)p^2} + x^{a_2+a_0p+a_1p^2}y^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2}$$

$$+2x^{(a_0+a_2)+(a_1+a_0)p+(a_2+a_1)p^2}y^{(a_0+a_1)+(a_1+a_2)p+(a_2+a_0)p^2} + x^{(2a_0+a_2)+(2a_1+a_0)p+(2a_2+a_1)p^2}y^{a_1+a_2p+a_0p^2}$$

A more complex example

$S = p+1$, $n = (a_2a_1a_0)_p$, $2 \le a_0, a_1 \le a_2$, $a_2 > (p+1)/2$ and $t = 2+p+p^2$

$$
\begin{aligned}
f_n^t(x) = {} & \\
& x^{(2+a_1)+(2+a_2)p+(2+a_0)p^2} + 2x^{2+2p+2p^2}y^{a_0+a_1p+a_2p^2} + x^{(a_2+a_1)+(a_0+a_2)p+(a_0+a_1)p^2}y^{2a_0+2a_1p+2a_2p^2} \\
& + x^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2}y^{a_2+a_0p+a_1p^2} + 2x^{(a_0+a_1)+(a_1+a_2)p+(a_2+a_0)p^2}y^{(a_0+a_2)+(a_1+a_0)p+(a_2+a_1)p^2} \\
& + x^{a_1+a_2p+a_0p^2}y^{(2a_0+a_2)+(2a_1+a_0)p+(2a_2+a_1)p^2} + y^{(2+a_1)+(2+a_2)p+(2+a_0)p^2} + 2x^{a_0+a_1p+a_2p^2}y^{2+2p+2p^2} \\
& + x^{2a_0+2a_1p+2a_2p^2}y^{(a_1+a_2)+(a_0+a_2)p+(a_0+a_1)p^2} + x^{a_2+a_0p+a_1p^2}y^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2} \\
& + 2x^{(a_0+a_2)+(a_1+a_0)p+(a_2+a_1)p^2}y^{(a_0+a_1)+(a_1+a_2)p+(a_2+a_0)p^2} + x^{(2a_0+a_2)+(2a_1+a_0)p+(2a_2+a_1)p^2}y^{a_1+a_2p+a_0p^2}
\end{aligned}
$$

A more complex example

$S = p + 1$, $n = (a_2 a_1 a_0)_p$, $2 \leq a_0, a_1 \leq a_2$, $a_2 > (p+1)/2$ and $t = 2 + p + p^2$

$$f_n^t(x) =$$

$$x^{(2+a_1)+(2+a_2)p+(2+a_0)p^2} + 2x^{2+2p+2p^2}y^{a_0+a_1p+a_2p^2} + x^{(a_2+a_1)+(a_0+a_2)p+(a_0+a_1)p^2}y^{2a_0+2a_1p+2a_2p^2}$$

$$+x^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2}y^{a_2+a_0p+a_1p^2} + 2x^{(a_0+a_1)+(a_1+a_2)p+(a_2+a_0)p^2}y^{(a_0+a_2)+(a_1+a_0)p+(a_2+a_1)p^2}$$

$$+x^{a_1+a_2p+a_0p^2}y^{(2a_0+a_2)+(2a_1+a_0)p+(2a_2+a_1)p^2} + y^{(2+a_1)+(2+a_2)p+(2+a_0)p^2} + 2x^{a_0+a_1p+a_2p^2}y^{2+2p+2p^2}$$

$$+x^{2a_0+2a_1p+2a_2p^2}y^{(a_1+a_2)+(a_0+a_2)p+(a_0+a_1)p^2} + x^{a_2+a_0p+a_1p^2}y^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2}$$

$$+2x^{(a_0+a_2)+(a_1+a_0)p+(a_2+a_1)p^2}y^{(a_0+a_1)+(a_1+a_2)p+(a_2+a_0)p^2} + x^{(2a_0+a_2)+(2a_1+a_0)p+(2a_2+a_1)p^2}y^{a_1+a_2p+a_0p^2}$$

$$x^{(2a_0+a_2)+(2a_1+a_0)p+(p+1+a_2-a_0)p^2}y^{a_1+a_2p+a_0p^2} = x^{(2a_0+a_2+1)+(2a_1+a_0)p+(a_2-a_0+1)p^2}y^{a_1+a_2p+a_0p^2}$$

A more complex example

$S = p+1$, $n = (a_2 a_1 a_0)_p$, $2 \le a_0, a_1 \le a_2$, $a_2 > (p+1)/2$ and $t = 2 + p + p^2$

$$f_n^t(x) =$$

$$x^{(2+a_1)+(2+a_2)p+(2+a_0)p^2} + 2x^{2+2p+2p^2}y^{a_0+a_1p+a_2p^2} + x^{(a_2+a_1)+(a_0+a_2)p+(a_0+a_1)p^2}y^{2a_0+2a_1p+2a_2p^2}$$

$$+x^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2}y^{a_2+a_0p+a_1p^2} + 2x^{(a_0+a_1)+(a_1+a_2)p+(a_2+a_0)p^2}y^{(a_0+a_2)+(a_1+a_0)p+(a_2+a_1)p^2}$$

$$+x^{a_1+a_2p+a_0p^2}y^{(2a_0+a_2)+(2a_1+a_0)p+(2a_2+a_1)p^2} + y^{(2+a_1)+(2+a_2)p+(2+a_0)p^2} + 2x^{a_0+a_1p+a_2p^2}y^{2+2p+2p^2}$$

$$+x^{2a_0+2a_1p+2a_2p^2}y^{(a_1+a_2)+(a_0+a_2)p+(a_0+a_1)p^2} + x^{a_2+a_0p+a_1p^2}y^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2}$$

$$+2x^{(a_0+a_2)+(a_1+a_0)p+(a_2+a_1)p^2}y^{(a_0+a_1)+(a_1+a_2)p+(a_2+a_0)p^2} + x^{(2a_0+a_2)+(2a_1+a_0)p+(2a_2+a_1)p^2}y^{a_1+a_2p+a_0p^2}$$

A more complex example

$S = p+1$, $n = (a_2 a_1 a_0)_p$, $2 \le a_0, a_1 \le a_2$, $a_2 > (p+1)/2$ and $t = 2 + p + p^2$

$$
\begin{aligned}
f_n^t(x) = \\
& x^{(2+a_1)+(2+a_2)p+(2+a_0)p^2} + 2x^{2+2p+2p^2} y^{a_0+a_1p+a_2p^2} + x^{(a_2+a_1)+(a_0+a_2)p+(a_0+a_1)p^2} y^{2a_0+2a_1p+2a_2p^2} \\
& + x^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2} y^{a_2+a_0p+a_1p^2} + 2x^{(a_0+a_1)+(a_1+a_2)p+(a_2+a_0)p^2} y^{(a_0+a_2)+(a_1+a_0)p+(a_2+a_1)p^2} \\
& + x^{a_1+a_2p+a_0p^2} y^{(2a_0+a_2)+(2a_1+a_0)p+(2a_2+a_1)p^2} + y^{(2+a_1)+(2+a_2)p+(2+a_0)p^2} + 2x^{a_0+a_1p+a_2p^2} y^{2+2p+2p^2} \\
& + x^{2a_0+2a_1p+2a_2p^2} y^{(a_1+a_2)+(a_0+a_2)p+(a_0+a_1)p^2} + x^{a_2+a_0p+a_1p^2} y^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2} \\
& + 2x^{(a_0+a_2)+(a_1+a_0)p+(a_2+a_1)p^2} y^{(a_0+a_1)+(a_1+a_2)p+(a_2+a_0)p^2} + x^{(2a_0+a_2)+(2a_1+a_0)p+(2a_2+a_1)p^2} y^{a_1+a_2p+a_0p^2}
\end{aligned}
$$

$$C_1 = \binom{a_2+a_1}{a_2+2}\binom{a_1+a_0}{a_1+2}\binom{a_0+a_2}{a_0+2} \quad C_2 = \binom{a_2+a_0}{a_2+2}\binom{a_1+a_2}{a_1+2}\binom{a_0+a_1}{a_0+2}$$

A more complex example

$S = p + 1$, $n = (a_2 a_1 a_0)_p$, $2 \leq a_0, a_1 \leq a_2$, $a_2 > (p+1)/2$ and $t = 2 + p + p^2$

$$f_n^t(x) =$$
$$x^{(2+a_1)+(2+a_2)p+(2+a_0)p^2} + 2x^{2+2p+2p^2} y^{a_0+a_1 p+a_2 p^2} + x^{(a_2+a_1)+(a_0+a_2)p+(a_0+a_1)p^2} y^{2a_0+2a_1 p+2a_2 p^2}$$
$$+x^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2} y^{a_2+a_0 p+a_1 p^2} + 2x^{(a_0+a_1)+(a_1+a_2)p+(a_2+a_0)p^2} y^{(a_0+a_2)+(a_1+a_0)p+(a_2+a_1)p^2}$$
$$+x^{a_1+a_2 p+a_0 p^2} y^{(2a_0+a_2)+(2a_1+a_0)p+(2a_2+a_1)p^2} + y^{(2+a_1)+(2+a_2)p+(2+a_0)p^2} + 2x^{a_0+a_1 p+a_2 p^2} y^{2+2p+2p^2}$$
$$+x^{2a_0+2a_1 p+2a_2 p^2} y^{(a_1+a_2)+(a_0+a_2)p+(a_0+a_1)p^2} + x^{a_2+a_0 p+a_1 p^2} y^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2}$$
$$+2x^{(a_0+a_2)+(a_1+a_0)p+(a_2+a_1)p^2} y^{(a_0+a_1)+(a_1+a_2)p+(a_2+a_0)p^2} + x^{(2a_0+a_2)+(2a_1+a_0)p+(2a_2+a_1)p^2} y^{a_1+a_2 p+a_0 p^2}$$

$$C_1 = \binom{a_2+a_1}{a_2+2}\binom{a_1+a_0}{a_1+2}\binom{a_0+a_2}{a_0+2} \quad C_2 = \binom{a_2+a_0}{a_2+2}\binom{a_1+a_2}{a_1+2}\binom{a_0+a_1}{a_0+2}$$

$$C_{tot} = 2C_1 + 2C_2 = 4C_1 \not\equiv 0 \bmod p$$

Example [No. 10]

$n = 2p + (p-1)p^2$ and $t = 2 + (p-1)p$ $(m = \frac{p-1}{2})$

$$
\begin{aligned}
f_n(x)^t =& (y^n - x^n)^2 (y^n - x^n)^{(p-1)p} \\
=& A_1 - 2A_2 + A_3 \\
A_1 =& \sum_{i=0}^{p-1} y^{(p-i+2)+(i+3)p+(2i-2)p^2} x^{(i+1)+(p-i-2)p+(2p-2i-2)p^2} \\
A_2 =& \sum_{i=0}^{p-1} y^{(p-i+1)+(i+1)p+(2i-1)p^2} x^{(i+2)+(p-i)p+(2p-2i-3)p^2} \\
A_3 =& \sum_{i=0}^{p-1} y^{(p-i)+(i-1)p+2ip^2} x^{(i+3)+(p-i+2)p+(2p-2i-4)p^2}
\end{aligned}
$$

A_1 only with $i = m, m+1$, so $c_1 = \ldots = \frac{-(m+3)(m+2)^2(m+1)m}{2 \cdot 4!}$;

A_2 only with $i = m$, so $c_2 = \ldots = \frac{-(m+2)(m+1)^2 m^2 (m-1)}{4!}$;

A_3 only with $i = m-1, m$, so $c_3 = \ldots = c_1$.

In total $C_{tot} = 2c_1 - 2c_2 = \frac{m(m+1)(m+2)}{2 \cdot 4!}(-3) \not\equiv 0 \mod p$.

The most challenging case [No. 7]

$n = 1 + 2p + (p-2)p^2$ and $t = (p-1) + (p-1)p$

The most challenging case [No. 7]

$n = 1 + 2p + (p-2)p^2$ and $t = (p-1) + (p-1)p$

$$\begin{aligned} f_n^t(x) =& (y^n - x^n)^t = (y^n - x^n)^{p-1}(y^n - x^n)^{(p-1)p} \\ =& \sum_{i,j=0}^{p-1} x^{4p^2-4p-ni-njp} y^{ni+njp} \end{aligned}$$

The most challenging case [No. 7]

$n = 1 + 2p + (p-2)p^2$ and $t = (p-1) + (p-1)p$

$$f_n^t(x) = (y^n - x^n)^t = (y^n - x^n)^{p-1}(y^n - x^n)^{(p-1)p}$$
$$= \sum_{i,j=0}^{p-1} x^{4p^2-4p-ni-njp} y^{ni+njp} = \sum_{i,j} x^{\alpha} y^{\beta}$$

The most challenging case [No. 7]

$n = 1 + 2p + (p-2)p^2$ and $t = (p-1) + (p-1)p$

$$\begin{aligned} f_n^t(x) =& (y^n - x^n)^t = (y^n - x^n)^{p-1}(y^n - x^n)^{(p-1)p} \\ =& \sum_{i,j=0}^{p-1} x^{4p^2-4p-ni-njp} y^{ni+njp} = \sum_{i,j} x^{\alpha} y^{\beta} \end{aligned}$$

Set $w = i + j$,

$$\begin{aligned} \alpha =& (4j - 2w) + p(p - (2w+4)) + p^2(2w + 3 - 4j) \\ \beta =& (2w - 4j) + 2pw + p^2(4j - 2w) \end{aligned}$$

The most challenging case [No. 7]

For $0 \le i \le 3$ set $s_i = \sum_{j=0}^{k} \binom{4j+i}{3}$ with k largest s.t. $4k + i < p$

$$
\begin{array}{rl}
\text{if } w < (p-3)/2 & \mathit{coeff} = 0 \\
\text{if } w = (p-3)/2 & \mathit{coeff} = -3s_3 + s_r \text{ with } r = 3 - (p \mod 4) \\
\text{if } w = (p-1)/2 & \mathit{coeff} = -s_1 + 3s_r \text{ with } r = (p \mod 4) - 1 \\
\text{if } (p-1)/2 < w < p-2 & \mathit{coeff} = 0 \\
\text{if } w = p-2 & \mathit{coeff} = -3s_1 + 1 + s_r - 1 \text{ with } r = (p \mod 4) - 1 \\
\text{if } w = p-1 & \mathit{coeff} = -s_3 + 3s_r - 3s_1 + s_{2-r} \text{ with } r = 3 - (p \mod 4) \\
\text{if } w = p & \mathit{coeff} = -s_3 + 3s_r \text{ with } r = 3 - (p \mod 4) \\
\text{if } p < w < p + (p-3)/2 & \mathit{coeff} = 0 \\
\text{if } w = p + (p-3)/2 & \mathit{coeff} = -3s_3 + s_r \text{ with } r = 3 - (p \mod 4) \\
\text{if } w = p + (p-1)/2 & \mathit{coeff} = -s_1 + 3s_r \text{ with } r = (p \mod 4) - 1 \\
\text{if } w > p + (p-1)/2 & \mathit{coeff} = 0
\end{array}
$$

The most challenging case [No. 7]

For $0 \leq i \leq 3$ set $s_i = \sum_{j=0}^{k} \binom{4j+i}{3}$ with k largest s.t. $4k + i < p$

$$
\begin{array}{rl}
\text{if } w < (p-3)/2 & coeff = 0 \\
\text{if } w = (p-3)/2 & coeff = -3s_3 + s_r \text{ with } r = 3 - (p \mod 4) \\
\text{if } w = (p-1)/2 & coeff = -s_1 + 3s_r \text{ with } r = (p \mod 4) - 1 \\
\text{if } (p-1)/2 < w < p-2 & coeff = 0 \\
\text{if } w = p-2 & coeff = -3s_1 + 1 + s_r - 1 \text{ with } r = (p \mod 4) - 1 \\
\text{if } w = p-1 & coeff = -s_3 + 3s_r - 3s_1 + s_{2-r} \text{ with } r = 3 - (p \mod 4) \\
\text{if } w = p & coeff = -s_3 + 3s_r \text{ with } r = 3 - (p \mod 4) \\
\text{if } p < w < p + (p-3)/2 & coeff = 0 \\
\text{if } w = p + (p-3)/2 & coeff = -3s_3 + s_r \text{ with } r = 3 - (p \mod 4) \\
\text{if } w = p + (p-1)/2 & coeff = -s_1 + 3s_r \text{ with } r = (p \mod 4) - 1 \\
\text{if } w > p + (p-1)/2 & coeff = 0
\end{array}
$$

In total $C_{tot} = \sum coeff = 8 \sum_{k=3}^{p-1} (-1)^k \binom{k}{3} = \ldots = -1$

Some references

R.S. Coulter, *The classification of planar monomials over fields of prime square order*, Proc. Amer. Math. Soc. **134** (2006), 3373–3378.

R.S. Coulter, E. Bergman and I. Villa, *Classifying planar monomials over fields of order a prime cubed*, Finite Fields and Their Applications 78 (2022): 101959.

R.S. Coulter and F. Lazebnik, *On the classification of planar monomials over fields of square order*, Finite Fields Appl. **18** (2012), 316–336.

R.S. Coulter and R.W. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr. **10** (1997), 167–184.

P. Dembowski and T.G. Ostrom, *Planes of order n with collineation groups of order* n^2, Math. Z. **103** (1968), 239–258.

D. Gluck, *Affine planes and permutation polynomials*, Coding Theory and Design Theory, part II (Design Theory), The IMA Volumes in Mathematics and its Applications, vol. 21, Springer-Verlag, 1990, pp. 99–100.

C. Hermite, *Sur les fonctions de sept lettres*, C.R. Acad. Sci. Paris **57** (1863), 750–757.

Y. Hiramine, *A conjecture on affine planes of prime order*, J. Combin. Theory Ser. A **52** (1989), 44–50.

N.L. Johnson, *Projective planes of order p that admit collineation groups of order* p^2, J. Geometry **30** (1987), 49–68.

E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math **1** (1878), 184–240, 289–321.

L. Rónyai and T. Szőnyi, *Planar functions over finite fields*, Combinatorica **9** (1989), 315–320.

M.E. Zieve, *Planar functions and perfect nonlinear monomials over finite fields*, Des. Codes Cryptogr. **75** (2015), 71–80.

Thank you for your attention