On quasi-planar monomials over finite fields

Mohit Pal

(joint work with S.U. Hasan, C. Riera and P. Stănică)

University of Bergen, Norway

mohit.pal@uib.no

April 22, 2024

Table of contents

Notations and definitions

- We denote, by $\mathbb{F}_q$, the finite field with $q = p^n$ elements, where p is a prime number and n is a positive integer.

Notations and definitions

- We denote, by $\mathbb{F}_q$, the finite field with $q = p^n$ elements, where p is a prime number and n is a positive integer.
- By $\mathbb{F}_q^* = \langle g \rangle$, we denote the multiplicative cyclic group of nonzero elements of $\mathbb{F}_q$, where g is a primitive element of $\mathbb{F}_q$.

Notations and definitions

- We denote, by $\mathbb{F}_q$, the finite field with $q = p^n$ elements, where p is a prime number and n is a positive integer.
- By $\mathbb{F}_q^* = \langle g \rangle$, we denote the multiplicative cyclic group of nonzero elements of $\mathbb{F}_q$, where g is a primitive element of $\mathbb{F}_q$.
- Let f be a function form the finite field $\mathbb{F}_q$ to itself then f can be uniquely represented as a univariate polynomial over $\mathbb{F}_q$ of the form

$$f(X) = \sum_{i=0}^{q-1} a_i X^i, \ a_i \in \mathbb{F}_q.$$

Notations and definitions

- We denote, by $\mathbb{F}_q$, the finite field with $q = p^n$ elements, where p is a prime number and n is a positive integer.
- By $\mathbb{F}_q^* = \langle g \rangle$, we denote the multiplicative cyclic group of nonzero elements of $\mathbb{F}_q$, where g is a primitive element of $\mathbb{F}_q$.
- Let f be a function form the finite field $\mathbb{F}_q$ to itself then f can be uniquely represented as a univariate polynomial over $\mathbb{F}_q$ of the form
$$f(X) = \sum_{i=0}^{q-1} a_i X^i,\ a_i \in \mathbb{F}_q.$$
- We call a polynomial $f \in \mathbb{F}_q[X]$, a permutation polynomial (PP) over $\mathbb{F}_q$ if the associated mapping $x \mapsto f(x)$ is a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$.

Difference Distribution Table

- One of the most important developments in block cipher cryptanalysis was the invention of differential cryptanalysis by Biham and Shamir[1].

[1] Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)

Difference Distribution Table

- One of the most important developments in block cipher cryptanalysis was the invention of differential cryptanalysis by Biham and Shamir[1].
- Let f be a function from $\mathbb{F}_q$ to itself.

[1] Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)

Difference Distribution Table

- One of the most important developments in block cipher cryptanalysis was the invention of differential cryptanalysis by Biham and Shamir[1].
- Let f be a function from $\mathbb{F}_q$ to itself.
- For any $a \in \mathbb{F}_q$, the derivative of f in the direction of a is defined as

$$D_f(a) := f(X + a) - f(X),$$

for all $X \in \mathbb{F}_q$.

[1] Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)

Difference Distribution Table

- One of the most important developments in block cipher cryptanalysis was the invention of differential cryptanalysis by Biham and Shamir[1].
- Let f be a function from $\mathbb{F}_q$ to itself.
- For any $a \in \mathbb{F}_q$, the derivative of f in the direction of a is defined as

$$D_f(a) := f(X+a) - f(X),$$

  for all $X \in \mathbb{F}_q$.
- For any $a, b \in \mathbb{F}_q$, the difference distribution table (DDT) entry of f at point (a, b) is defined as

$$\Delta_f(a,b) := |\{X \in \mathbb{F}_q \mid f(X+a) - f(X) = b\}|.$$

[1] Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)

Difference Distribution Table

- One of the most important developments in block cipher cryptanalysis was the invention of differential cryptanalysis by Biham and Shamir[1].
- Let f be a function from $\mathbb{F}_q$ to itself.
- For any $a \in \mathbb{F}_q$, the derivative of f in the direction of a is defined as

$$D_f(a) := f(X+a) - f(X),$$

  for all $X \in \mathbb{F}_q$.
- For any $a, b \in \mathbb{F}_q$, the difference distribution table (DDT) entry of f at point (a, b) is defined as

$$\Delta_f(a, b) := |\{X \in \mathbb{F}_q \mid f(X+a) - f(X) = b\}|.$$

- The differential uniformity of f, denoted by Δ_f, is given by

$$\Delta_f := \max\{\Delta_f(a, b) \mid a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\}.$$

[1] Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)

Differential Uniformity

- Thus, a function f is called differentially Δ_f-uniform if for every $a \in \mathbb{F}_q^*$ and every $b \in \mathbb{F}_q$, the equation $f(X+a) - f(X) = b$ admits at most Δ_f solutions.

Differential Uniformity

- Thus, a function f is called differentially Δ_f-uniform if for every $a \in \mathbb{F}_q^*$ and every $b \in \mathbb{F}_q$, the equation $f(X+a) - f(X) = b$ admits at most Δ_f solutions.
- When $\Delta_f = 1$, we say that the function f is perfect nonlinear (PN) function (or **planar function**).

Differential Uniformity

- Thus, a function f is called differentially Δ_f-uniform if for every $a \in \mathbb{F}_q^*$ and every $b \in \mathbb{F}_q$, the equation $f(X+a) - f(X) = b$ admits at most Δ_f solutions.
- When $\Delta_f = 1$, we say that the function f is perfect nonlinear (PN) function (or **planar function**).
- When $\Delta_f = 2$, we say that the function f is almost perfect nonlinear (APN) function.

Extended Difference Distribution Table

- In 2020, Ellingsen et al.[2] extentended the notion of the differential unifomity.

[2] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity*, IEEE Trans. Inform. Theory 66:9 (2020), 5781–5789.

Extended Difference Distribution Table

- In 2020, Ellingsen et al.[2] extentended the notion of the differential unifomity.
- For any $a, c \in \mathbb{F}_q$, the c-derivative of f in the direction of a is defined as

$$ {}_cD_f(a) := f(X + a) - cf(X), $$

for all $X \in \mathbb{F}_q$.

[2] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity*, IEEE Trans. Inform. Theory 66:9 (2020), 5781–5789.

Extended Difference Distribution Table

- In 2020, Ellingsen et al.[2] extentended the notion of the differential unifomity.
- For any $a, c \in \mathbb{F}_q$, the c-derivative of f in the direction of a is defined as
$$ {}_cD_f(a) := f(X+a) - cf(X), $$
for all $X \in \mathbb{F}_q$.
- For any $a, b, c \in \mathbb{F}_q$, the c-difference distribution table (DDT) entry of f at point (a, b) is defined as
$$ {}_c\Delta_f(a,b) = |\{X \in \mathbb{F}_q \mid f(X+a) - cf(X) = b\}|. $$

[2] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity*, IEEE Trans. Inform. Theory 66:9 (2020), 5781–5789.

c-Differential Uniformity

- The c-differential uniformity of f, denoted by ${}_c\Delta_f$, is given by

$$ {}_c\Delta_f = \max\{{}_c\Delta_f(a, b) \mid a, b \in \mathbb{F}_q \text{ and } a \neq 0 \text{ if } c = 1\}. $$

c-Differential Uniformity

- The c-differential uniformity of f, denoted by ${}_c\Delta_f$, is given by

$$ {}_c\Delta_f = \max\{{}_c\Delta_f(a,b) \mid a, b \in \mathbb{F}_q \text{ and } a \neq 0 \text{ if } c = 1\}. $$

- When ${}_c\Delta_f = 1$, we say that the function f is perfect c-nonlinear (PcN) function (or c-**planar function**).

c-Differential Uniformity

- The c-differential uniformity of f, denoted by ${}_c\Delta_f$, is given by

$$ {}_c\Delta_f = \max\{{}_c\Delta_f(a,b) \mid a, b \in \mathbb{F}_q \text{ and } a \neq 0 \text{ if } c = 1\}. $$

- When ${}_c\Delta_f = 1$, we say that the function f is perfect c-nonlinear (PcN) function (or c-**planar function**).
- When p is odd and $c = -1$ then we call a c-planar function, **quasi-planar**.

c-Differential Uniformity

- The c-differential uniformity of f, denoted by ${}_c\Delta_f$, is given by

$$ {}_c\Delta_f = \max\{{}_c\Delta_f(a, b) \mid a, b \in \mathbb{F}_q \text{ and } a \neq 0 \text{ if } c = 1\}. $$

- When ${}_c\Delta_f = 1$, we say that the function f is perfect c-nonlinear (PcN) function (or c-**planar function**).
- When p is odd and $c = -1$ then we call a c-planar function, **quasi-planar**.
- When ${}_c\Delta_f = 2$, we say that the function f is almost perfect c-nonlinear (APcN) function.

Facts

- A function f is planar if and only if $f(X+a)-f(X)$ is a permutation polynomial for all $a \in \mathbb{F}_q^*$.

Facts

- A function f is planar if and only if $f(X+a)-f(X)$ is a permutation polynomial for all $a \in \mathbb{F}_q^*$.
- A permutation polynomial can never be a planar function.

Facts

- A function f is planar if and only if $f(X+a)-f(X)$ is a permutation polynomial for all $a \in \mathbb{F}_q^*$.
- A permutation polynomial can never be a planar function.
- A function f is quasi-planar if and only if $f(X+a)+f(X)$ is a permutation polynomial for all $a \in \mathbb{F}_q$.

Facts

- A function f is planar if and only if $f(X + a) - f(X)$ is a permutation polynomial for all $a \in \mathbb{F}_q^*$.
- A permutation polynomial can never be a planar function.
- A function f is quasi-planar if and only if $f(X + a) + f(X)$ is a permutation polynomial for all $a \in \mathbb{F}_q$.
- If a function f is quasi-planar then it has to be a permutation polynomial.

Well-known classes of PPs

- A monomial X^d is a permutation polynomial over $\mathbb{F}_q$ if and only if $\gcd(d, q-1) = 1$.

Well-known classes of PPs

- A monomial X^d is a permutation polynomial over $\mathbb{F}_q$ if and only if $\gcd(d, q-1) = 1$.
- A linearized polynomial over $\mathbb{F}_q$ is a polynomial of the form

$$f(X) = \sum_{i=0}^{n-1} a_i X^{p^i} \in \mathbb{F}_{p^n}[X].$$

Well-known classes of PPs

- A monomial X^d is a permutation polynomial over $\mathbb{F}_q$ if and only if $\gcd(d, q-1) = 1$.
- A linearized polynomial over $\mathbb{F}_q$ is a polynomial of the form

$$f(X) = \sum_{i=0}^{n-1} a_i X^{p^i} \in \mathbb{F}_{p^n}[X].$$

- A linearized polynomial is a permutation polynomial if and only if 0 is its only root in $\mathbb{F}_q$.

Dickson Polynomial

- We recall the Dickson's original approach of defining the Dickson polynomial $D_d(X, a)$, where d is a positive integer and $a \in \mathbb{F}_q$.

Dickson Polynomial

- We recall the Dickson's original approach of defining the Dickson polynomial $D_d(X, a)$, where d is a positive integer and $a \in \mathbb{F}_q$.
- In fact, the d-th Dickson polynomial of the first kind $D_d(X, a)$ admits the following representation

$$\begin{aligned} u_1^d + u_2^d &= \sum_{i=0}^{\lfloor \frac{d}{2} \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-u_1 u_2)^i (u_1 + u_2)^{d-2i} \\ &= D_d(u_1 + u_2, u_1 u_2), \end{aligned} \qquad (1)$$

where u_1, u_2 are indeterminates and

$$D_d(X, a) = \sum_{i=0}^{\lfloor \frac{d}{2} \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-a)^i X^{d-2i}.$$

Dickson Polynomial

- We recall the Dickson's original approach of defining the Dickson polynomial $D_d(X,a)$, where d is a positive integer and $a \in \mathbb{F}_q$.
- In fact, the d-th Dickson polynomial of the first kind $D_d(X,a)$ admits the following representation

$$\begin{aligned} u_1^d + u_2^d &= \sum_{i=0}^{\lfloor \frac{d}{2} \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-u_1u_2)^i (u_1+u_2)^{d-2i} \\ &= D_d(u_1+u_2, u_1u_2), \end{aligned} \tag{1}$$

where u_1, u_2 are indeterminates and

$$D_d(X,a) = \sum_{i=0}^{\lfloor \frac{d}{2} \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-a)^i X^{d-2i}.$$

- A Dickson polynomial $D_d(X,a)$ is a permutation polynomial if and only if $\gcd(d, q^2-1) = 1$.

Quasi-planar monomials

Lemma (HPRS)

A monomial X^d is quasi-planar in $\mathbb{F}_{p^n}$ if and only if X^d and $(X+1)^d + (X-1)^d$ are permutations of $\mathbb{F}_{p^n}$.

Proof: For $a \neq 0$, $(X+a)^d + X^d$ is a permutation of $\mathbb{F}_{p^n}$ if and only if

$$a^d \left[\left(\frac{X}{a} + 1 \right)^d + \left(\frac{X}{a} \right)^d \right] \text{ is a permutation of } \mathbb{F}_{p^n}$$

$$\iff \quad \left(\frac{X}{a} + 1 \right)^d + \left(\frac{X}{a} \right)^d \text{ is a permutation of } \mathbb{F}_{p^n}$$

$$\iff \quad (y+1)^d + y^d \text{ is a permutation of } \mathbb{F}_{p^n}; \text{ where } ay = X$$

$$\iff \quad \left(\frac{2y+1+1}{2} \right)^d + \left(\frac{2y+1-1}{2} \right)^d \text{ is a permutation of } \mathbb{F}_{p^n}$$

$$\overset{z:=2y+1}{\iff} \quad \left(\frac{1}{2} \right)^d \left[(z+1)^d + (z-1)^d \right] \text{ is a permutation of } \mathbb{F}_{p^n}$$

$$\iff \quad (z+1)^d + (z-1)^d \text{ is a permutation of } \mathbb{F}_{p^n}.$$

Quasi-planar monomials and Dickson polynomials

Theorem (HPRS)

Let p be an odd prime, d be a positive integer such that

$$d = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$$

for some $k \geq 0$, where $a_i \in \{0, 1, \cdots, p-1\}$ and $a_0, a_k \neq 0$, then

$$(X+1)^d + (X-1)^d = 2D_d(X, \epsilon)$$

for some $\epsilon \in \mathbb{F}_p^*$ if and only if either

(1) $d = 1, 2, 3$; or

(2) $a_0 = \dfrac{p+1}{2}$ and $a_j = \dfrac{p-1}{2}$ $\forall j \in \{1, 2, \ldots, k\}$ $\left(\text{i.e., } d = \dfrac{p^{k+1}+1}{2}\right)$.

Theorem (HPRS)

The power map $X^{\frac{p^\ell+1}{2}}$ is a permutation of $\mathbb{F}_{p^n}$ if and only if any one of the following conditions hold:

(1) $\ell = 0$;

(2) ℓ is even and n is odd;

(3) ℓ is even and n is even together with $t_2 \geq t_1$, where $n = 2^{t_1} u$ and $\ell = 2^{t_2} v$ such that $2 \nmid u, v$;

(4) ℓ is odd, n is odd and $p \equiv 1 \pmod 4$.

Theorem (HPRS)

If both ℓ, n are odd and $p \equiv 1 \pmod 4$, then the power map $X^{\frac{p^\ell+1}{2}}$ is not quasi-planar over $\mathbb{F}_{p^n}$.

Proof: Since ℓ is odd and $p \equiv 1 \pmod 4$, $\dfrac{p^\ell+1}{2}$ is odd. Notice that

$$
\begin{aligned}
& X^{\frac{p^\ell+1}{2}} \text{ is PcN over } \mathbb{F}_{p^n} \\
\iff & (X+1)^{\frac{p^\ell+1}{2}} + (X-1)^{\frac{p^\ell+1}{2}} \text{ is a permutation of } \mathbb{F}_{p^n} \\
\iff & D_{\frac{p^\ell+1}{2}}\left(X, \frac{1}{4}\right) \text{ is a permutation of } \mathbb{F}_{p^n}, \forall\ 1 \le \ell < n \\
\iff & \gcd\left(\frac{p^\ell+1}{2}, p^{2n}-1\right) = 1 \\
\iff & \gcd\left(p^\ell+1, p^{2n}-1\right) = 2 \\
\iff & \frac{2n}{\gcd(\ell, 2n)} \text{ is odd.}
\end{aligned}
$$

But since ℓ and n are odd, $\dfrac{2n}{\gcd(\ell, 2n)}$ is never odd and we are done.

Theorem (HPRS)

The power map $X^{\frac{p^\ell+1}{2}}$ is quasi-planar over $\mathbb{F}_{p^n}$ if and only if any one of the following conditions holds:

(1) $\ell = 0$;

(2) ℓ even and n odd;

(3) ℓ even and n even together with $t_2 \geq t_1 + 1$, where $n = 2^{t_1} u$ and $\ell = 2^{t_2} v$ such that $2 \nmid u, v$.

Quasi-planar monomials over $\mathbb{F}_p$

In 2020, Bartoli and Timpanella [3] proved the following theorem.

Theorem (BT)

Let $d \in \{0, 1, \ldots, p-1\}$. Then the monomial X^d is quasi-planar over $\mathbb{F}_p$ if and only if $d = 1$.

[3] D. Bartoli, M. Timpanella, *On a generalization of planar functions*, J. Algebr. Comb. 52 (2020),187–213.

In 2020, Bartoli and Timpanella [4] proved the following theorem.

Theorem (BT)

Let

$$d \in \left\{ p^i, p^i(p^2 - p + 1), p^i\left(\frac{p^2+1}{2}\right) : i = 0, 1, 2 \right\}.$$

Then the monomial X^d is quasi-planar over $\mathbb{F}_{p^3}$.

[4] D. Bartoli, M. Timpanella, *On a generalization of planar functions*, J. Algebr. Comb. 52 (2020),187–213.

Open Problem

Conjecture (Bartoli and Timpanella)

Let p be an odd prime. Then the monomial X^d is quasi-planar over $\mathbb{F}_{p^3}$ if and only if

$$d \in \left\{ p^i, p^i(p^2 - p + 1), p^i \left(\frac{p^2+1}{2} \right) : i = 0, 1, 2 \right\}.$$

Thank you for your attention!