The differential properties of certain permutation polynomials over finite fields

Sartaj Ul Hasan

Department of Mathematics
Indian Institute of Technology Jammu
sartaj.hasan@iitjammu.ac.in

Algebraic and Combinatorial Methods for Coding and Cryptography

Marseille, France
February 20-24, 2023

(Joint work with K. Garg and P. Stănică.)

Outline

- Notations and definitions
- Differential Uniformity
- Multiplicative Differentials
- The c-differential uniformity
- Our contributios

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.
- $\mathbb{F}_q^*$ denote the multiplicative cyclic group of nonzero elements of $\mathbb{F}_q$.
- We call a polynomial $f \in \mathbb{F}_q[X]$, a permutation polynomial over $\mathbb{F}_q$ if the associated mapping $X \mapsto f(X)$ is a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$.
- We shall use Tr_m^n to denote the (relative) trace function from $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, i.e., $\mathrm{Tr}_m^n(X) = \sum_{i=0}^{\frac{n-m}{m}} X^{p^{mi}}$, where m and n are positive integers and $m|n$. When $m = 1$, we use Tr to denote the absolute trace.
- By $v_p(n)$, we denote the highest non-negative exponent ν such that p^ν divides n (that is, the p-adic valuation).

Additive character and Weil sum

Definition

The canonical additive character is a homomorphism $\chi_1 : \mathbb{F}_q \to \mathbb{C}$ of the additive group of $\mathbb{F}_q$ defined as follows

$$\chi_1(X) := \exp\left(\frac{2\pi i \operatorname{Tr}(X)}{p}\right),$$

where $\mathbb{C}$ is the field of complex numbers and $\operatorname{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the absolute trace defined by $\operatorname{Tr}(X) = X + X^p + X^{p^2} + \cdots + X^{p^{n-1}}$.

Additive character and Weil sum

Definition

The canonical additive character is a homomorphism $\chi_1 : \mathbb{F}_q \to \mathbb{C}$ of the additive group of $\mathbb{F}_q$ defined as follows

$$\chi_1(X) := \exp\left(\frac{2\pi i \operatorname{Tr}(X)}{p}\right),$$

where $\mathbb{C}$ is the field of complex numbers and $\operatorname{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the absolute trace defined by $\operatorname{Tr}(X) = X + X^p + X^{p^2} + \cdots + X^{p^{n-1}}$.

Definition

Let χ be an additive character of $\mathbb{F}_q$ and $f(X)$ is a polynomial in $\mathbb{F}_q[X]$. Then the Weil sum of the function f is defined as follows

$$\sum_{X \in \mathbb{F}_q} \chi(f(X)).$$

Characters and Equations over Finite Fields

- The canonical additive character over finite fields of characteristic p can be written as

$$\chi_1(X) = \omega^{\mathrm{Tr}(X)},$$

where $\omega = e^{\frac{2\pi i}{p}}$ is a complex primitive p^{th} root of unity.

- The number of solutions $(X_1, X_2, \ldots, X_n) \in \mathbb{F}_q^n$ of the equation $f(X_1, X_2, \ldots, X_n) = b$, is given by

$$\frac{1}{q} \sum_{X_1, X_2, \ldots, X_n \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} \chi_1(\beta(f(X_1, X_2, \ldots, X_n) - b)),$$

or equivalently,

$$\frac{1}{q} \sum_{X_1, X_2, \ldots, X_n \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} \omega^{\mathrm{Tr}(\beta(f(X_1, X_2, \ldots, X_n) - b))}.$$

Walsh transform

Definition

For a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_p$, the Walsh transform of F at $v \in \mathbb{F}_{p^n}$, is defined as

$$\mathcal{W}_F(v) := \sum_{X \in \mathbb{F}_{p^n}} \omega^{F(X) - \mathrm{Tr}(vX)},$$

where $\omega = e^{\frac{2\pi i}{p}}$ is a complex primitive pth root of unity.

Differential uniformity

- Substitution boxes play a very crucial role in the design of secure cryptographic primitives, such as block ciphers.
- Differential attack, introduced by E. Biham and A. Shamir[1] is one of the most efficient attacks on the substitution boxes used in the block cipher.
- To quantify the degree of security of a substitution box, against the differential attack, K. Nyberg[2] introduced the notion of differential uniformity (DU).

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

[2] K. Nyberg, *Differentially uniform mappings for cryptography.* In: Helleseth T. (eds.), Advances in Cryptology–EUROCRYPT 1993, LNCS 765, Springer, Berlin, Heidelberg, pp. 55–64, 1994.

Differential uniformity

Definition

For any function $f : \mathbb{F}_q \to \mathbb{F}_q$ and $a \in \mathbb{F}_q$, the derivative of f in the direction a, denoted by $D_f(X, a)$, is defined as

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

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

Differential uniformity

Definition

For any function $f : \mathbb{F}_q \to \mathbb{F}_q$ and $a \in \mathbb{F}_q$, the derivative of f in the direction a, denoted by $D_f(X, a)$, is defined as

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

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

Definition

For any $a, b \in \mathbb{F}_q$, the Difference Distribution Table (DDT) entry at point (a, b), denoted by $\Delta_f(a, b)$, is defined as

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

Differential uniformity

Definition

The differential uniformity of f, denoted by Δ_f, is defined as

$$\Delta_f := \max\{\Delta_f(a, b) \mid a, b \in \mathbb{F}_q, a \neq 0\}.$$

Differential uniformity

Definition

The differential uniformity of f, denoted by Δ_f, is defined as

$$\Delta_f := \max\{\Delta_f(a, b) \mid a, b \in \mathbb{F}_q, a \neq 0\}.$$

- When $\Delta_f = \delta$, we say that the function f is δ-uniform.

Differential uniformity

Definition

The differential uniformity of f, denoted by Δ_f, is defined as

$$\Delta_f := \max\{\Delta_f(a, b) \mid a, b \in \mathbb{F}_q, a \neq 0\}.$$

- When $\Delta_f = \delta$, we say that the function f is δ-uniform.
- When $\delta = 1$, we say that the function f is perfect nonlinear (PN) function.

Differential uniformity

Definition

The differential uniformity of f, denoted by Δ_f, is defined as

$$\Delta_f := \max\{\Delta_f(a, b) \mid a, b \in \mathbb{F}_q, a \neq 0\}.$$

- When $\Delta_f = \delta$, we say that the function f is δ-uniform.
- When $\delta = 1$, we say that the function f is perfect nonlinear (PN) function.
- When $\delta = 2$, we say that the function f is almost perfect nonlinear (APN) function.

Multiplicative differentials

- In 2002, N. Borisov, M. Chew, R. Johnson, D. Wagner[3] introduced the notion of multiplicative differentials of the form $(f(cX), f(X))$ and used this new type of differentials to attack some existing ciphers.

[3] N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative differentials*. In: J. Daemen and V. Rijmen (eds.) Proceedings of Fast Software Encryption - FSE 2002. Lecture Notes in Comput. Sci., Springer, Berlin, Heidelberg, vol. 2365 (2002), 17–33.

[4] 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.

Multiplicative differentials

- In 2002, N. Borisov, M. Chew, R. Johnson, D. Wagner[3] introduced the notion of multiplicative differentials of the form $(f(cX), f(X))$ and used this new type of differentials to attack some existing ciphers.

- In 2020, P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko[4] defined a new (output) multiplicative differential given in the next slide.

---

[3] N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative differentials*. In: J. Daemen and V. Rijmen (eds.) Proceedings of Fast Software Encryption - FSE 2002. Lecture Notes in Comput. Sci., Springer, Berlin, Heidelberg, vol. 2365 (2002), 17–33.

[4] 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.

The c-differential uniformity

Definition (Ellingsen-Felke-Riera-Stănică-Tkachenko, 2020)

For any function F from a finite field $\mathbb{F}_q$ to itself and for any $a, c \in \mathbb{F}_q$, the (multiplicative) c-derivative of F with respect to a is defined as

$$_cD_F(X, a) := F(X + a) - cF(X) \text{ for all } X \in \mathbb{F}_q.$$

The c-differential uniformity

Definition (Ellingsen-Felke-Riera-Stănică-Tkachenko, 2020)

For any function F from a finite field $\mathbb{F}_q$ to itself and for any $a, c \in \mathbb{F}_q$, the (multiplicative) c-derivative of F with respect to a is defined as

$$_cD_F(X, a) := F(X + a) - cF(X) \text{ for all } X \in \mathbb{F}_q.$$

Definition

For $a, b \in \mathbb{F}_q$, the c-Difference Distribution Table (cDDT) entry of F at point (a, b), denoted by $_c\Delta_F(a, b)$, is given by

$$_c\Delta_F(a, b) := |\{X \in \mathbb{F}_q : \ _cD_F(X, a) = b\}|.$$

The c-differential uniformity

Definition (Ellingsen-Felke-Riera-Stănică-Tkachenko, 2020)

The c-differential uniformity (cDU) of F, denoted as ${}_c\Delta_F$, is defined as

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

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

The c-differential uniformity

Definition (Ellingsen-Felke-Riera-Stănică-Tkachenko, 2020)

The c-differential uniformity (cDU) of F, denoted as ${}_c\Delta_F$, is defined as

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

- If $c = -1$: quasi-planar, Bartoli and Timpanela[5] (discovered independently).
- If ${}_c\Delta_F = \delta$: F is (c,δ)-uniform.

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

The c-differential uniformity

Definition (Ellingsen-Felke-Riera-Stănică-Tkachenko, 2020)

The c-differential uniformity (cDU) of F, denoted as ${}_c\Delta_F$, is defined as

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

- If $c = -1$: quasi-planar, Bartoli and Timpanela[5] (discovered independently).
- If ${}_c\Delta_F = \delta$: F is (c,δ)-uniform.
- If ${}_c\Delta_F = 1$: F is perfect c-nonlinear (PcN) function (certainly, for $c = 1$, they only exist for odd p; if $c \neq 1$, there exist PcN functions for all p).

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

The c-differential uniformity

Definition (Ellingsen-Felke-Riera-Stănică-Tkachenko, 2020)

The c-differential uniformity (cDU) of F, denoted as ${}_c\Delta_F$, is defined as

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

- If $c = -1$: quasi-planar, Bartoli and Timpanela[5] (discovered independently).
- If ${}_c\Delta_F = \delta$: F is (c,δ)-uniform.
- If ${}_c\Delta_F = 1$: F is perfect c-nonlinear (PcN) function (certainly, for $c = 1$, they only exist for odd p; if $c \neq 1$, there exist PcN functions for all p).
- If ${}_c\Delta_F = 2$: F is almost perfect c-nonlinear (APcN) function.
- $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is PcN $\iff$ ${}_cD_F$ is a permutation polynomial.

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

- Many teams started researching these notions: Bartoli, Calderini, Geary, H., C. Li, N. Li, Mesnager, Pal, Riera, Stănică., Yan, Wang, Wu, Zeng, Zheng, Zhou, etc.

- Characterizations of the c-differential uniformity; some of the known perfect and almost perfect nonlinear functions have been investigated; constructions, etc.

The c-differential uniformity for Gold, CM & Inverse

Ellingsen-Felke-Riera-Stănică-Tkachenko[6], 2020

- X^2: APcN, for all $c \neq 1$.
- $X^{p^k+1}, p > 2$ is never PcN, for all $c \neq 1$; Oddly, when $(1-c)^{p^k-1} = 1$ and $n/\gcd(n,k)$ is even, then ${}_c\Delta_F \geq p^g + 1$,where $g = \gcd(n,k)$.
- If $X^{\frac{3^k+1}{2}}$ over $\mathbb{F}_{3^n}$ is PcN, for $c = -1 \iff \frac{2n}{\gcd(2n,k)}$ is odd.
- Inverse $F(X) = X^{2^n-2}$ over $\mathbb{F}_{2^n}$: APcN if $\mathrm{Tr}_n(c) = \mathrm{Tr}_n(1/c) = 1$; Otherwise, ${}_c\Delta_F = 3, c \neq 0$;
- Inverse $F(X) = X^{p^n-2}$ over $\mathbb{F}_{p^n}, p$ odd: APcN if $c \neq 0, (c^2-4c)$ and $(1-4c) \notin (\mathbb{F}_{p^n})^2$; Otherwise, ${}_c\Delta_F = 3, c \neq 0$.

---

[6] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity,* IEEE Trans. Inf. Theory 66:6 (2020), 5781–5789.

The c-differential uniformity of the Gold function

Mesnager-Riera-Stănică.-Yan-Zhou[7], 2021

Let $2 \leq k < n, n \geq 3$ and $G(X) = X^{2^k+1}$ Gold function over $\mathbb{F}_{2^n}, 1 \neq c \in \mathbb{F}_{2^n}$. Under some condition, ${}_c\Delta_G = 2^d + 1, d = \gcd(n, k)$ (if $d = 1$, no extra conditions are required).

[7] S. Mesnager, C. Riera, P. Stănică, H. Yan, and Z. Zhou, *Investigations on c-(Almost) Perfect Nonlinear Functions*, IEEE Trans. Inf. Theory 67:10 (2021), 6916–6925.

Bartoli-Calderini[8], 2021

- We recall that Dembowski-Ostrom (DO) polynomials over a finite field $\mathbb{F}_q$ are those of the form

$$\sum_{i,j} a_{ij} X^{p^i+p^j}, \quad \text{where } a_{ij} \in \mathbb{F}_q.$$

- If f is a quadratic polynomial over $\mathbb{F}_{p^m}$, and $1 \neq c \in \mathbb{F}_p$, then f is permutation polynomial iff f is PcN. Further, if f is Dembowski-Ostrom (DO), then f is APcN iff f is planar.

[8] D. Bartoli, M. Calderini, *On construction and (non)existence of c-(almost) perfect nonlinear functions*,Finite Fields Appl. 72 (2021), 101835

H.-Pal-Riera-Stănică[9], 2021

Conjecture 1

Let p be an odd prime.Then, for $c = -1$, and for all $0 \leq j \leq 4$,

$$p^j \left\{ 1, \frac{p^2+1}{2}, p^4 + (p-2)p^2 + (p-1)p + 1, \frac{p^4+1}{2}, \frac{p^5+1}{p+1} \right\}$$

are the only values of d for which x^d is PcN on $\mathbb{F}_{p^5}$.

[9] S. U. Hasan, M. Pal, C. Riera, P. Stănică, *On the c-differential uniformity of certain maps over finite fields*, Des. Codes Cryptogr. 89 (2021), 221–239.

H.-Pal-Riera-Stănică[10], 2021

Conjecture 2

Let p be an odd prime. Then for $c = -1$ and for all $0 \leq j \leq 6$,

$$p^j \Bigg\{1, \frac{p^2+1}{2}, ((p-1)p^6 + p^5 + (p-2)p^3 + (p-1)p^2 + p), \frac{p^4+1}{2}, \\ \frac{p^6+1}{2}, (p-2)p^6 + (p-2)p^5 + (p-1)p^4 + p^3 + p^2 + p, \frac{p^7+1}{p+1}\Bigg\}$$

are the only values of d for which x^d is PcN over $\mathbb{F}_{p^7}$.

[10] S. U. Hasan, M. Pal, C. Riera, P. Stănică, *On the c-differential uniformity of certain maps over finite fields*, Des. Codes Cryptogr. 89 (2021), 221–239.

We first recall a lemma by K. S. Williams [11] dealing with solutions of a cubic equation over a finite field with even characteristic.

Lemma

For a positive integer n and $a \in \mathbb{F}_{2^n}^*$, the cubic equation $X^3 + X + a = 0$ has

1. a unique solution in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(a^{-1} + 1) = 1$;
2. three distinct solutions in $\mathbb{F}_{2^n}$ if and only if $p_n(a) = 0$, where the polynomial $p_n(X)$ is recursively defined by the equations $p_1(X) = p_2(X) = X, p_k(X) = p_{k-1}(X) + X^{2^{k-3}} p_{k-2}(X)$ for $k \geq 3$;
3. no solutions in $\mathbb{F}_{2^n}$, otherwise.

[11] K. S. Williams, *Note on cubics over $GF(2^n)$ and $GF(3^n)$*, J. Number Theory 7:4 (1975), 361–365.

- There are very few known classes of PcN functions over binary field.

[12] Z. Zha and L. Hu, *Some classes of permutation polynomials of the form* $(x^{p^m} - x + \delta)^s + x$ *over* $\mathbb{F}_{p^{2m}}$, Finite Fields Appl. 40, 2016, 150–162.

- There are very few known classes of PcN functions over binary field.
- Our aim is to find more classes of permutations with low c-differential uniformity.

[12] Z. Zha and L. Hu, *Some classes of permutation polynomials of the form* $(x^{p^m} - x + \delta)^s + x$ *over* $\mathbb{F}_{p^{2m}}$, Finite Fields Appl. 40, 2016, 150–162.

- There are very few known classes of PcN functions over binary field.
- Our aim is to find more classes of permutations with low c-differential uniformity.

In 2016, Z. Zha and L. Hu[12] proposed the following class of permutation polynomials over $\mathbb{F}_{2^{2m}}$

Lemma

Let m be a positive integer and $p_m(X)$ be same as defined in previous lemma. Let $\delta \in \mathbb{F}_{2^{2m}}$ satisfies either $\delta \in \mathbb{F}_{2^m}$, or $\delta \notin \mathbb{F}_{2^m}$ with $\mathrm{Tr}_1^{2m}(\delta) = \mathrm{Tr}_1^m(1)$ and $p_m((\delta + \bar{\delta})^{-1}) \neq 0$. The polynomial

$$G_1(X) = (X^{2^m} + X + \delta)^{2^{2m-2}+2^{m-2}+1} + X$$

permutes $\mathbb{F}_{2^{2m}}$.

[12] Z. Zha and L. Hu, *Some classes of permutation polynomials of the form* $(x^{p^m} - x + \delta)^s + x$ *over* $\mathbb{F}_{p^{2m}}$, Finite Fields Appl. 40, 2016, 150–162.

Result

We have computed c-differential uniformity of five classes of permutation polynomials. In particular we give four classes of PcN functions over binary fields.

Theorem 1 (First class)

Let $G_1(X) = (X^{2^m} + X + \delta)^{2^{2m-2}+2^{m-2}+1} + X$ over $\mathbb{F}_{2^n}$, where $n = 2m$.

1. Let $\delta \in \mathbb{F}_{2^m}$. Then G_1 is PcN for $c \in \mathbb{F}_{2^m} \setminus \{1\}$. Moreover, G_1 is APcN for $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$.
2. Let $\delta \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ with $\mathrm{Tr}_1^{2m}(\delta) = \mathrm{Tr}_1^m(1)$ and $p_m((\delta + \bar{\delta})^{-1}) \neq 0$, where $p_m(X)$ is the polynomial defined in the above Lemma. Then G_1 is PcN for $c \in \mathbb{F}_{2^m} \setminus \{1\}$ and is of c-differential uniformity ≤ 4 for $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$.

Idea of the proof

- We know that the c-DDT entry ${}_c\Delta_{G_1}(a, b)$ at the point (a, b) of the function $G_1(X)$ is given by the number of solutions $X \in \mathbb{F}_q$ of the equation $G_1(X + a) + cG_1(X) = b$, or equivalently,

$$\begin{aligned}(1+c)G_1(X) + \mathrm{Tr}_m^{2m}(\mathrm{Tr}_m^{2m}(a^{2^{m-1}})X + a\mathrm{Tr}_m^{2m}(X^{2^{m-1}})) + G_1(a) \\ + \mathrm{Tr}_m^{2m}(\delta^{2^{m-2}})\mathrm{Tr}_m^{2m}(\mathrm{Tr}_m^{2m}(a^{2^{m-2}})X + a\mathrm{Tr}_m^{2m}(X^{2^{m-2}})) \\ = b + \delta^{2^{2m-2}+2^{m-2}+1}.\end{aligned}$$

Idea of the proof

- We know that the c-DDT entry ${}_c\Delta_{G_1}(a,b)$ at the point (a,b) of the function $G_1(X)$ is given by the number of solutions $X \in \mathbb{F}_q$ of the equation $G_1(X+a)+cG_1(X)=b$, or equivalently,

$$(1+c)G_1(X)+\mathrm{Tr}_m^{2m}(\mathrm{Tr}_m^{2m}(a^{2^{m-1}})X+a\mathrm{Tr}_m^{2m}(X^{2^{m-1}}))+G_1(a)$$
$$+\mathrm{Tr}_m^{2m}(\delta^{2^{m-2}})\mathrm{Tr}_m^{2m}(\mathrm{Tr}_m^{2m}(a^{2^{m-2}})X+a\mathrm{Tr}_m^{2m}(X^{2^{m-2}}))$$
$$=b+\delta^{2^{2m-2}+2^{m-2}+1}.$$

- Thus, the # of solutions $X \in \mathbb{F}_q$, ${}_c\Delta_{G_1}(a,b)$, is given by

$$\frac{1}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}}(\beta(G_1(a)+b+\delta^{2^{2m-2}+2^{m-2}+1}))\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(1+c)G_1}$$
$$(-1)^{\mathrm{Tr}(\beta(\mathrm{Tr}_m^{2m}(\delta^{2^{m-2}})\mathrm{Tr}_m^{2m}((a^{2^{m-2}}+a^{2^{2m-2}})X+a(X^{2^{m-2}}+X^{2^{2m-2}})}$$
$$(-1)^{\mathrm{Tr}(\beta(\mathrm{Tr}_m^{2m}((a^{2^{m-1}}+a^{2^{2m-1}})X+a(X^{2^{m-1}}+X^{2^{2m-1}}))))}.$$

Second class of PcN functions over binary fields

Another class of permutation polynomials Z. Zha and L. Hu[13] proposed over $\mathbb{F}_{2^{2m}}$ for a positive integer $m \not\equiv 0 \pmod 3$ and any element $\delta \in \mathbb{F}_{2^{2m}}$, is $G_2(X) = (X^{2^m} + X + \delta)^{3\cdot 2^{2m-2}+2^{m-2}} + X$.

Theorem 2 (Second Class)

Let $G_2(X) = (X^{2^m} + X + \delta)^{3\cdot 2^{2m-2}+2^{m-2}} + X$ over $\mathbb{F}_{2^n}$, where $n = 2m$ and $m \not\equiv 0 \pmod 3$. Then G_2 is PcN for all $c \in \mathbb{F}_{2^m} \setminus \{1\}$ and $\delta \in \mathbb{F}_{2^n}$.

[13] Z. Zha and L. Hu, *Some classes of permutation polynomials of the form* $(x^{p^m} - x + \delta)^s + x$ *over* $\mathbb{F}_{p^{2m}}$, Finite Fields Appl.(2016) 40, 150–162.

Third class of PcN functions over binary fields

Next, we considered a class of permutation polynomials given by L. Wang, W. Baofeng, and L. Zhuojun[14] over the finite field $\mathbb{F}_{2^{2m}}$. The authors showed that for a positive integer $m \not\equiv 0 \pmod 3$ and any element $\delta \in \mathbb{F}_{2^{2m}}$, the polynomial $G_3(X) = (X^{2^m} + X + \delta)^{3\cdot 2^{m-2}+2^{2m-2}} + X$ permutes $\mathbb{F}_{2^{2m}}$.

Theorem 3 (Third Class)

Let $G_3(X) = (X^{2^m} + X + \delta)^{3\cdot 2^{m-2}+2^{2m-2}} + X$ over $\mathbb{F}_{2^n}$, where $n = 2m$ and $m \not\equiv 0 \pmod 3$. Then G_3 is PcN for all $c \in \mathbb{F}_{2^m} \setminus \{1\}$ and $\delta \in \mathbb{F}_{2^n}$.

[14] L. Wang, W. Baofeng, and L. Zhuojun, *Further results on permutation polynomials of the form* $(X^{p^m} - X + \delta)^s + L(X)$ *over* $\mathbb{F}_{p^{2m}}$, Finite Fields Appl. 44 (2017), 92–112

Some more classes of permutation polynomials

L. Li, S. Wang, C. Li, and X. Zeng [15] showed that the following classes of polynomials are permutations over finite fields.

- $G_4(X) = (X^{2^m} + X + \delta)^{2^{2m+1}+2^m} + (X^{2^m} + X + \delta)^{2^{2m}+2^{m+1}} + X$ is a permutation of $\mathbb{F}_{2^n}$ where $\delta \in \mathbb{F}_{2^{3m}}$ with $\mathrm{Tr}_m^n(\delta) = 0$ and $n = 3m$.

- $G_5(X) = (X^{3^m} - X + \delta)^{3^m+4} + (X^{3^m} - X + \delta)^5 + X$ is a permutation of $\mathbb{F}_{3^{2m}}$, where $\delta \in \mathbb{F}_{3^{2m}}$ and $(1 - [\mathrm{Tr}_m^{2m}(\delta)])$ is a square element in $\mathbb{F}_{3^m}$.

[15] L. Li, S. Wang, C. Li, and X. Zeng, *Permutation polynomials* $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + x$ *over* $\mathbb{F}_{p^n}$, Finite Fields Appl. 51 (2018), 31–61.

Results

Theorem 4 (Fourth Class)

Let $G_4(X) = (X^{2^m} + X + \delta)^{2^{2m+1}+2^m} + (X^{2^m} + X + \delta)^{2^{2m}+2^{m+1}} + X$ over $\mathbb{F}_{2^n}$, where $n = 3m$. Let $\delta \in \mathbb{F}_{2^n}$ and $\mathrm{Tr}_m^{3m}(\delta) = 0$. Then G_4 is PcN for $c \in \mathbb{F}_{2^m} \setminus \{1\}$.

Theorem 5 (Fifth Class)

Let $G_5(X) = (X^{3^m} - X + \delta)^{3^m+4} + (X^{3^m} - X + \delta)^5 + X$ over $\mathbb{F}_{3^n}$, where $n = 2m$ and $\delta \in \mathbb{F}_{3^n}$ such that $(1 - [\mathrm{Tr}_m^{2m}(\delta)]^4)$ is a square element in $\mathbb{F}_{3^m}^*$. Then:

1. G_5 is PcN for all $c \in \mathbb{F}_{3^m} \setminus \{1\}$.
2. Moreover, G_5 is of c-differential uniformity 3 for all $c \in \mathbb{F}_{3^n} \setminus \mathbb{F}_{3^m}$.

Conclusions

i. We investigate the c-differential uniformity of some classes of permutation polynomials.

ii. In particular, we add four more classes of permutation polynomials to the class that only contains a few perfect c-nonlinear functions over finite fields of even characteristic.

iii. We have used various techniques including Walsh transforms, Weil sums and a very detailed analysis of the involved equations.

Thank you for your attention!