A NOTE ON PERFECT NONLINEAR FUNCTIONS OVER FINITE FIELDS OF ODD CHARACTERISTIC

Dhananjay Kumar[1], Rajesh P. Singh[2*], Rishi Kumar Jha[3]

Abstract

A polynomial f over a finite field $\mathbb{F}_q$ is called a permutation polynomial if its associate function $f: \mathbb{F}_q \to \mathbb{F}_q$ is a bijective mapping. If $f(x+a) - f(x)$ is a permutation polynomial of $\mathbb{F}_q$ for every $a \in \mathbb{F}_q^*$, then the polynomial $f(x)$ is said to be perfect nonlinear or planar. Perfect nonlinear functions are closely related to permutation polynomials. In this article we propose a class of perfect nonlinear function over $\mathbb{F}_{q^4}$. We also characterize a family of DO-polynomials of the form $\sum_{i,j=0}^{n-1} a_{ij} x^{q^i+q^j}$ to be perfect nonlinear function over $\mathbb{F}_{q^n}$.

[1,3]Department of Mathematics, National Institute of Technology Patna, India.
[2*]Department of Mathematics, Central University of South Bihar, Gaya, India.

***Corresponding Author: -** Rajesh P. Singh
[*]Department of Mathematics, Central University of South Bihar, Gaya, India.
Email:- rpsingh@cub.ac.in

DOI: 10.48047/ecb/2023.12.si10.0027

Introduction

Let p be a prime, $q = p^m$ and $\mathbb{F}_q$ be a finite field with q elements. A polynomial $h(x)$ over finite field $\mathbb{F}_q$ is called a permutation polynomial of $\mathbb{F}_q$ if the map $h : \mathbb{F}_q \to \mathbb{F}_q$ is a bijective function.

Permutation polynomials have been studied for over a century and have variety of applications in Coding theory [6], Cryptography [17,18], and Combinatorics [19] and in other branches of mathematics and engineering. Fernando studied some special type of permutation binomials and trinomials over finite fields [11]. Gong et al. investigated the permutation polynomials of the form $x^{2^k+1} + L(x)$ [12]. Jarali et al. constructed some classes of permutation polynomials and planar functions [13].

The derivative of a real or complex valued function is a useful tool when studying various mathematical and physical phenomena. The derivative of a differentiable function at a given point provides the best affine approximation of the function. For functions defined over finite fields the notion of derivative takes a different appearance and is closely related to designs and combinatorial structures. The discrete derivative of $f(x)$ at a point $\theta \in F_q^*$ is defined as:

$$\mathfrak{D}_\theta(h(x)) = h(x + \theta) - h(x)$$

A polynomial $f \in \mathbb{F}_q[x]$ is called planar function or perfect nonlinear (PN) function if for every nonzero $\theta \in \mathbb{F}_q$, the discrete derivative is a permutation polynomial over $\mathbb{F}_q$. P. Dembowski and T. G. Ostrom introduced the idea of planar functions in 1968 [10]. They used such functions to investigate the projective planes with some specific properties. Planar functions have a wide range of applications in Combinatorics [3], Cryptography [4], Coding theory [5] and many other branches of mathematics.

Bartoli and Bonini Characterized a family of planar trinomials of the form $xL(x)$ where $L(x)$ is a linearized polynomial over $\mathbb{F}_{q^3}$[2]. In 2008, Coulter and Henderson [8] studied the Commutative presemifields and semifields in connection with perfect nonlinear functions and proved some fundamental results. In 2012, Coulter [7] obtained a complete classification of planar monomials over fields of order p^4. Coulter and Matthews investigated the projective geometry using perfect nonlinear functions and produced a non-DO-type example of PN function in [9]. Interested readers can see the reference [16] for an excellent survey on planar functions by Pott.

Let $\mathfrak{D}_\theta(h(x)) = h(x + \theta) - h(x) = \delta$ has $n(\theta, \delta)$ numbers of solutions for some $\delta, \theta \in \mathbb{F}_q$. Consider $\Delta_h = max\{n(\delta, \theta): \theta, \delta \in \mathbb{F}_q, \theta \neq 0\}$. If $\Delta_h = m$ then the function h is called differentially m −uniform. Functions with least differential uniformity have applications in Cryptography. It is evident that planar functions if exists are differentially 1-uniform. Functions having differential uniformity 1 are also called Perfect Nonlinear (PN).

It is easy to note that if $p = 2$, then $+1 = -1$ and conscequently x and $x + \theta$ both are solutions of $\mathfrak{D}_\theta(h(x)) = \delta$. So, there is no planar function over the finite fields of even characteristic. The differential uniformity for any function over finite fields of even characteristic is greater than or equal to 2. Functions over finite fields of even characteristic with differential uniformity 2 are called Almost Perfect Nonlinear (APN) functions. APN functions are mainly used in Cryptography to resist the differential attacks on block ciphers.

In 2013 a new definition for planar function over even characteristic was given by Y. Zhou [21] while studying the relative difference sets. The modified definition is somewhat like the existing one.

Definition

A polynomial $h \in \mathbb{F}_{2^n}[x]$ is said to be a planar polynomial if $\mathfrak{D}_\theta(h(x)) = h(x + \theta) + h(x) + \theta x$ is a permutation polynomial of $\mathbb{F}_{2^n}$ for every $\theta \in \mathbb{F}_{2^n}^*$.

To distinguish the new definition with existing one, Pott named such functions as Modified Planar [16], while Abdukhalikov [1] called them Pseudo Planar. These functions have many properties like their counter parts over odd characteristic. Such functions are used in construction of semifields, difference sets and other combinatorial objects [8,21]. The motive of this article is to investigate some classes of planar functions over finite fields of odd characteristic. We propose a class of planar function over $\mathbb{F}_{q^3}$ and characterise a polynomial of the form $\sum_{i,j=0}^{n-1} u_i u_j x^{q^i+q^j}$ to be a planar function over $\mathbb{F}_{q^n}$.

2. Some Preliminary results

It is well known that any function from finite field $\mathbb{F}_q$ to itself can be uniquely expressed as a polynomial of degree less than q using Langrarges interpolation formula. Moreover, polynomials with degree up to $q - 1$ determines a unique function of $\mathbb{F}_q$, see [11]. In this view, the set of functions of finite field $\mathbb{F}_q$ can be identified with the set of polynomials over $\mathbb{F}_q$ and vice-versa. If p is a prime number and k is a nonnegative integer, then the

p −weight of k is the sum of the digits in its p −adic representation, i.e., if $k = \sum b_i p^i$ then the p −ary weight of k is $\sum b_i$. The algebraic degree of a polynomial $f(x)$ is the largest p −ary weight of any exponent. The polynomials $\sum B_i\, x^{p^i} + C_i$ have algebraic degree 1. These polynomials are called affine polynomials.

Linearized Polynomials

A polynomial of the form $L(x) = \sum_0^{n-1} \alpha_i\, x^{q^i}, \alpha_i \in \mathbb{F}_{q^n}$ is called a linearized polynomial over $\mathbb{F}_{q^n}$.

One can see that linearized polynomials are additive in nature, that is, if $\alpha, \beta \in \mathbb{F}_{q^n}$ and $a \in \mathbb{F}_q$ then $L(a\alpha + \beta) = aL(\alpha) + L(\beta)$.

The next results characterize a linearized polynomial to be a permutation polynomial.

Lemma 1.[14]

Let $A = \begin{bmatrix} a_0 & {a_{n-1}}^q & \dots & {a_1}^{q^{n-1}} \\ a_1 & {a_0}^q & \dots & {a_2}^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & {a_{n-2}}^q & \dots & {a_0}^{q^{n-1}} \end{bmatrix}$

be a square matrix of order n with $a_i \in \mathbb{F}_{q^n}, 0 \le i \le n-1$. Then the linearized polynomial $L(x) = \sum_{i=0}^{n-1} a_i\, x^{q^i}$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if the matrix A is non-singular.

A matrix of the form $A = \begin{bmatrix} a_0 & a_{n-1} & \dots & a_1 \\ a_1 & a_0 & \dots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \dots & a_0 \end{bmatrix}$ is called a circulant matrix.

To determine the permutation behaviour of a linearized polynomial becomes easy if its coefficients are elements of first row of a circulant matrix. In the next result we present a fundamental result on invertibility of circulant matrix.

Lemma 2. [20]

Let $A = \begin{bmatrix} a_0 & a_{n-1} & \dots & a_1 \\ a_1 & a_0 & \dots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \dots & a_0 \end{bmatrix}$

Suppose $n = p^k$, then the circulant matrix A is non-singular if and only if $\sum_{i=0}^{n-1} a_i \neq 0$.

Dembowski-Ostrom Polynomial

The polynomials with algebraic degree 2 must be of the form $\sum A_i\, x^{q^i+q^j} + L(x) + C_i$ where $L(x)$ is a linearized polynomial. If we remove linear and constant terms then a polynomial of the form $\sum_{i,j} a_{ij}\, x^{p^i+p^j}$is called a Dembowski-Ostrom polynomial or DO-polynomial.

These polynomials are usually referred as DO-polynomials. It is quite interesting to note that all planar and pseudo planar functions known so far are DO-Polynomial with the only exception the monomial $x^{\frac{3^t+1}{2}}$, over finite field $\mathbb{F}_{3^n}$, where t is odd, and $\gcd(t, n) = 1$ [9]. It is easy to see that the monomial $x^{(3^t+1)/2}$ not of DO type. It is an open problem to construct a planar or pseudo planar functions other than DO-type [7,15,16].

Lemma 3. [9]

The discrete derivative of a Dembowski-Ostrom polynomial is a linearized polynomial.

3. Families of Planar Functions

In this section we study two families of DO-type planar functions. One of the family is a polynomial with five terms over $\mathbb{F}_{q^3}$. The other family is of the form $\sum_{i,j=0}^{q^{n-1}} u_i\, u_j x^{q^i+q^j}\, over\ \mathbb{F}_{q^n}$.

Theorem 1.

Let $u_{ii} = u_{3i} = u_{i3} = 1$, for $0 \le i \le 1\ and\ u_{i,j} = -1$ otherwise. Then the DO-polynomial $f(x) = \sum_{i,j=0}^{3} u_{ij}\, x^{p^{mi}+p^{mj}}$ is a perfect nonlinear function in $\mathbb{F}_{p^{4m}}$.

Proof:

We have $f(x) = x^2 - 2x^{p^m+1} - 2x^{p^{2m}+1} + 2x^{p^{3m}+1} + x^{2p^m} - 2x^{p^{2m}+p^m} + 2x^{p^{3m}+p^m} + x^{2p^{2m}} + 2x^{p^{2m}+p^{3m}} + x^{2p^{3m}}$. The discrete derivative of $f(x)$ at $b \in \mathbb{F}_{p^{4m}}^*$ is

$$\mathfrak{D}_b(f(x)) = f(x+b) - f(x) - f(b)$$

$$= \left(b - b^{p^m} - b^{p^{2m}} + b^{p^{3m}}\right)x + \left(-b + b^{p^m} - b^{p^{2m}} + b^{p^{3m}}\right)x^{p^m} + \left(-b - b^{p^m} + b^{p^{2m}} + b^{p^{3m}}\right)x^{p^{2m}} + \left(b + b^{p^m} + b^{p^{2m}} + b^{p^{3m}}\right)x^{p^{3m}}$$

$$= Tr(bx) + \left(-b^{p^m}x - b^{p^{2m}}x^{p^m} + b^{p^{3m}}x^{p^{2m}} + bx^{p^{3m}}\right) + \left(-b^{p^{2m}}x + b^{p^{3m}}x^{p^m} - bx^{p^{2m}} + b^{p^m}x^{p^{3m}}\right) + \left(b^{p^{3m}}x - bx^{p^m} - b^{p^m}x^{p^{2m}} + b^{p^{2m}}x^{p^{3m}}\right)$$

$$= Tr(bx) + Tr(b^{p^m}x) - 2(b^{p^m}x + b^{p^{2m}}x^{p^m}) + Tr(b^{p^{2m}}x)$$
$$-2(b^{p^{2m}}x + bx^{p^{2m}}) + Tr(b^{p^{3m}}x) - 2(bx^{p^m} + b^{p^m}x^{p^{2m}})$$
$$= Tr(b)Tr(x) - 2(b^{p^m}x + b^{p^{2m}}x^{p^m}) - 2(b^{p^{2m}}x + bx^{p^{2m}}) - 2(bx^{p^m} + b^{p^m}x^{p^{2m}})$$

Let u be a root of $\mathfrak{D}_b(f(x))$, that is, $\mathfrak{D}_b(f(u)) = 0$. It is sufficient to show that $u = 0$. On contrary, assume u is nonzero. Now we have,

$$Tr(\mathfrak{D}_b(f(u))) = 4Tr(b)Tr(u) - 2Tr\left(u(b^{p^m} + b^{p^{2m}})\right) + Tr\left(u^{p^m}(b + b^{p^{2m}})\right)$$
$$+Tr(u^{p^{2m}}(b + b^{p^m}))\}$$
$$= 4Tr(b)Tr(u) - 2\{Tr\left(u^{p^{2m}}(b^{p^{3m}} + b)\right) + Tr\left(u^{p^{2m}}(b^{p^m} + \ b^{p^{3m}})\right)$$
$$+Tr\left(u^{p^{2m}}(b + b^{p^m})\right)\}$$
$$= 4Tr(b)Tr(u) - 2Tr\left(2u^{p^{2m}}(b + b^{p^m} + b^{p^{3m}})\right)$$
$$= 4Tr(b)Tr(u) - 4\{Tr(u^{p^{2m}})Tr(b) - Tr(b^{p^{2m}}u^{p^{2m}})\}$$
$$= 4Tr(bu)$$

Since $\mathfrak{D}_b(f(u)) = 0$ implies $Tr(\mathfrak{D}_b(f(u))) = 0$. Therefore, we have $Tr(bu) = 0$. Since, u is nonzero and $b \in \mathbb{F}^*_{p^{4m}}$ is an arbitrary element. Therefore, bu represents an arbitrary element of $\mathbb{F}^*_{p^{4m}}$ with $Tr(bu) = 0$. This is a contradiction. Thus $\mathfrak{D}_b(f(u)) = 0$ implies $u = 0$.

In next result, we give necessary and sufficient condition for a family of DO-polynomial to be a planar polynomial.

Theorem 2.

The polynomial $f(x) = \sum_{i,j=0}^{n-1} u_i\, u_j x^{q^i+q^j}, u_i \in \mathbb{F}_q$ is a planar polynomial over $\mathbb{F}_{q^n}$ if and only if the matrix $\begin{bmatrix} u_0 & u_{n-1} & \cdots & u_1 \\ u_1 & u_0 & \cdots & u_2 \\ \vdots & \vdots & \ddots & \vdots \\ u_{n-1} & u_{n-2} & \cdots & u_0 \end{bmatrix}$ has rank n.

Proof:

$f(x) = \sum_{i,j=0}^{n-1} u_i\, u_j x^{q^i+q^j}$. The discrete derivative at any nonzero point $\theta \in \mathbb{F}_{q^n}$ is given by $\mathfrak{D}_\theta(f(x)) = f(x + \theta) - f(x) - f(\theta)$. We have,

$$\mathfrak{D}_\theta(f(x)) = \sum_{i,j=0}^{n-1} u_i\, u_j(x + \theta)^{q^i+q^j} - \sum_{i,j=0}^{n-1} u_i\, u_j x^{q^i+q^j} - \sum_{i,j=0}^{n-1} u_i\, u_j \theta^{q^i+q^j}$$
$$= \sum_{i,j=0}^{n-1} u_i\, u_j\left(x^{q^i+q^j} + x^{q^i}\theta^{q^j} + x^{q^j}\theta^{q^i} + \theta^{q^i+q^j}\right) - \sum_{i,j=0}^{n-1} u_i\, u_j x^{q^i+q^j}$$
$$-\sum_{i,j=0}^{n-1} u_i\, u_j \theta^{q^i+q^j}$$
$$= \sum_{i,j=0}^{n-1} u_i\, u_j\left(x^{q^i}\theta^{q^j} + x^{q^j}\theta^{q^i}\right)$$
$$= 2\sum_{i,j=0}^{n-1} u_i\, u_j x^{q^i}\theta^{q^j}$$
$$= 2\sum_{j=0}^{n-1} u_0\, u_j x\theta^{q^j} + 2\sum_{j=0}^{n-1} u_1\, u_j x^q\theta^{q^j} \cdots + 2\sum_{j=0}^{n-1} u_{n-1}\, u_j x^{q^{n-1}}\theta^{q^j}$$
$$= 2\sum_{i=0}^{n-1} u_i x^{q^i} . \sum_{j=0}^{n-1} u_j\, \theta^{q^j}$$

In view of $Lemma$ 2, we find that the linearized polynomial $\sum_{i=0}^{n-1} u_i x^{q^i}$ is a permutation polynomial and therefore, $\sum_{i=0}^{n-1} u_i b^{q^i} \neq 0$, for every $b \in \mathbb{F}_{q^n}^*$, consequently $\mathfrak{D}_\theta(f(x))$ is a permutation polynomial.

Corollary 1.
Let $n = p^k$, then $f(x) = \sum_{i,j=0}^{n-1} \beta_i \beta_j x^{p^i+p^j}$, $\beta_i \in \mathbb{F}_p$ is a planar polynomial over $\mathbb{F}_{p^n}$ if and only if $\sum_{i=0}^{n-1} \beta_i \neq 0$.

Proof:
The proof directly follows from *Theorem 2* and *Lemma 2.*

References:

1. K. Abdukhalikov, “Symplectic spreads, planar functions, and mutually unbiased bases,” J. Algebraic Comb., vol. 41 (2015). 1055-1077.
2. D. Bartoli, M. Bonini, Planar Polynomials arising from Linearized polynomials, J. Algebra Appl., 21(01) 2022, 2250002(18).
3. L. Budaghyan, T. Helleseth, New commutative semifields defined by new PN multinomials, Cryptogr. Commun. 3 (2011), 1–16.
4. C. Blondean, K. Nyberg, Perfect nonlinear functions and Cryptography, Finite Fields App.,32(2015), 120-147.
5. C. Carlet, C. Ding, J. Yuan, Linear codes from perfect nonlinear mappings and their secret sharing schemes, IEEE Trans. Inf. Theory, 51(6) (2005), 2089-2102.
6. Y. L. Chapuy, Permutation polynomials and applications to coding theory, Finite Fields App.,13 (2007), 58-70.
7. R. S. Coulter, On the classification of planar monomials over fields of square order, Finite Fields App., 18 (2012), 316-336.
8. R. S. Coulter, M. Henderson, Commutative presemifields and semifields, Advances in Mathematics, 217 (2008), 282-304.
9. R. S. Coulter, R. W. Matthews, Planar functions and planes of Lenz–Barlotti class II, Des. Codes Cryptogr., 10 (1997), 168-184.
10. P. Dembowski, T. G. Ostrom, Planes of order n with collineation groups of order n2, Math. Zeit., 103 (1968), 239-258.
11. N. Fernando, A note on permutation binomials and trinomials over finite fields, New Zeeland J. Math. 48(2018) 25-29
12. X. Gong, G. Gao, W. Liu, On permutation polynomials of the form $x^{2^k+1} + L(x)$ Int. J. Comput. Math. 93(10) (2016) 1715-1
13. V. Jarali, P. Poojary, VGR Bhatta. Construction of Permutation Polynomials Using Additive and Multiplicative Characters. Symmetry. 2022; 14(8):1539
14. R. Lidl, H. Niederreiter Finite Fields, Encyclopaedia of mathematics and its Applications, Cambridge University Press, 2003
15. G. L. Mullen, D. Panario, Handbook of Finite Fields, CRC Press, Taylor & Francis Group, 2013.
16. A. Pott, Almost perfect and planar functions, Des. Codes Cryptogr., 78 (2016), 141-195.
17. R. P. Singh, A. Saikia, B. K. Sarma. Poly-dragon: an efficient multivariate public key cryptosystem J. Math. Cryptol., 4(4), 2011, 349-364.
18. R. P. Singh, B. K. Sarma, A. Saikia. A Public Key Cryptosystem using a group of permutation polynomials, Tatra Mt. Math. Publ., 77 (2020), 139-162.
19. R. P. Singh, M. K. Singh Two congruence identities on ordered partitions, INTEGERS: Electronic journal of Combinatorial Number Theory, 18 (2018) A73.
20. R. P. Singh, Permutation polynomial and their applications in cryptography (Ph.D. Thesis) Indian Institute of Technology, Guwahati, 2010.
21. Y. Zhou, (2n, 2n, 2n, 1)-relative difference sets and their representations. J. Combin. Des.43(21), 563–584 (2013)