Palestine Journal of Mathematics

Vol 13(Special Issue II)(2024) , 50–57 © Palestine Polytechnic University-PPU 2024

Some Families of Planar functions over quadratic and cubic extensions of finite fields

Dhananjay Kumar, Rajesh P. Singh and Rishi Kumar Jha

Communicated by Manoj Kumar Patel

Dedicated to Prof. B. M. Pandeya on his 78th birthday

MSC 2020 Classification: Primary 11T06; Secondary 12K10.

Keywords and phrases: Planar functions, Perfect nonlinear functions, Permutation polynomials, Semifields.

Acknowledgement: The authors would like to thank the anonymous referees for their helpful comments.

Abstract A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is perfect nonlinear or planar if, for every nonzero $b \in \mathbb{F}_q$, the discrete derivative $f(x+b) - f(x) - f(b)$ of $f(x)$ is a bijection of $\mathbb{F}_q$. Perfect nonlinear functions have a wide range of applications in Combinatorics, Coding Theory, Finite Geometry, Cryptography, and Design Theory. A polynomial of the form $\sum_{i,j} a_{ij}x^{p^i+p^j}$ is called a Dembowski-Ostrom polynomial (DO polynomial). In this article, we construct four classes of perfect nonlinear functions of DO-type polynomials over finite fields $\mathbb{F}_{p^{tn}}$, for $t = 2$ and 3.

1 Introduction

Let $q = p^n$ and p be an odd prime. Let $\mathbb{F}_q$ be a finite field having q elements. A polynomial $\phi \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if the map $x \mapsto \phi(x)$ is a bijection. The problem of determining a permutation polynomial over a finite field is nontrivial. Permutation polynomials have been the subject of study for several years and have a wide range of applications in cryptography [24, 25], coding theory [11] and combinatorics [26]. The study of special types of permutation polynomials is an interesting problem, for instance see [1, 16, 10, 12, 22]. Some recent development on permutation polynomials can be found in [17, 15, 21, 3]. The polynomial $\phi(x)$ is called planar function or perfect nonlinear (PN) if the discrete derivative $\mathfrak{D}(\phi(x)) = \phi(x+a) - \phi(x) - \phi(a)$ is a permutation polynomial of $\mathbb{F}_q$ for every $a \in \mathbb{F}_q^*$. Let $\phi : \mathbb{F}_q \to \mathbb{F}_q$ be a function and define $\Delta_\phi = max \ \{n(\gamma,\delta) : \gamma,\delta \in \mathbb{F}_q; \gamma \neq 0\}$, where $n(\gamma,\delta)$ indicates the number of solutions of $\phi(x+\gamma) - \phi(x) = \delta$ for every $\gamma,\delta \in \mathbb{F}_q, \gamma \neq 0$. A function ϕ is defined as differentially d-uniform if $\Delta_\phi = d$. Due to their optimal resistance to differential cryptanalysis in Block ciphers, functions with low differential uniformity are given special attention for use in cryptography [5]. The functions which are differential 2-uniform are called almost perfect nonlinear (APN) functions over fields of characteristic 2. The differential 1-uniform functions are obviously perfect nonlinear or planar functions. The planar functions cannot exist over finite fields $\mathbb{F}_q$ of even characteristic. Since if q is even then both x and $x+a$ are solutions of $\phi(x+a) - \phi(x) = b$ for $b \in \mathbb{F}_q^*$. The planar functions initially appeared in the article of P. Dembowski and T.G. Ostrom in 1968 [13] where they used such functions to describe projective planes with specific properties. A polynomial of the form $\sum_{i,j} a_{ij}x^{p^i+p^j}$ is known as Dembowski-Ostrom polynomial or DO-type polynomial. It is interesting to note that all known classes of planar functions are of DO-type with the only exception $x^{\frac{3^s+1}{2}}$, s odd with $\gcd(s,n) = 1$ over finite field $\mathbb{F}_{3^n}$ [9]. It is conjectured that there is no planar functions other than DO-type over $\mathbb{F}_{p^n}$, for $p \geq 5$, [7, 20].

A commutative semifield is a nonassociative commutative ring without zero divisors and with an identity element. A commutative presemifield is a commutative semifield with the only exemption of having an identity element. No classification of finite commutative semifields exists yet, and very few classes of commutative semifields are known so far [8]. Planar DO polynomials are closely connected to commutative semifields and are used to construct new finite commutative semifields having odd order. Let $\phi(x)$ be a planar DO polynomial then we define a new operation $*$ on $\mathbb{F}_q$ by $x*y = \frac{1}{2}\{\phi(x+y)-\phi(x)-\phi(y)\}$. Now with the usual addition and $*$ as multiplication, $(\mathbb{F}_q, +, *)$ becomes a commutative presemifield. Given a presemifield, it is possible to define a new operation $\star$ which determines a semifield $(\mathbb{F}_q, +, \star)$ [8]. In this way, any finite commutative semifield can be determined by a planar DO polynomial over a finite field [4, 8]. Planar functions are also used in combinatorics for the construction of partial difference sets of Paley type, skew Hadamard difference sets [14] and in coding theory to construct linear and quasi-perfect linear codes [6, 18].

Two functions $\phi, \psi : \mathbb{F}_q \to \mathbb{F}_q$ are extended affine equivalent (EA-equivalent) if $\phi(x) = l_2(\psi(l_1(x))) + l_3(x)$ for bijective affine functions l_1, l_2 and l_3 of $\mathbb{F}_q$. The functions ϕ and ψ are Carlet-Charpin-Zinoviev equivalent (CCZ-equivalent) if the graphs of ϕ and ψ are affine equivalent [5]. It is proved in [4] that for perfect nonlinear functions over finite fields, EA-equivalence coincides with CCZ-equivalence. Finding new classes of inequivalent planar functions is a difficult problem. Only a handful of classes of perfect nonlinear functions are known so far [2].

As we see, perfect nonlinear functions have crucial applications in many mathematics disciplines. But only few classes of planar functions over finite fields of arbitrary odd characteristic are yet known. So, there is a solid motivation to find new families of perfect nonlinear functions. In this article, we find four classes of DO-type perfect nonlinear polynomials over finite fields $\mathbb{F}_{p^n}$, $n = 2m$ and $3m$ for any odd characteristic p. In section 3 of this paper, we present two classes of perfect nonlinear trinomials over quadratic extension. In section 4, we present two families of perfect nonlinear functions over cubic extension. Moreover, in the next Section (Section 2), we give the preliminary results required for the paper.

2 Preliminaries

Definition 2.1. Let $\mathbb{F}_{q^n}$ be the extension field of $\mathbb{F}_q$. A polynomial of the form $\mathfrak{L}(x) = \sum_{i=0}^{n-1} \delta_i x^{q^i}$, $\delta_i \in \mathbb{F}_{q^n}$, is called a linearized polynomial over $\mathbb{F}_{q^n}$.

It easily follows that linearized polynomials are additive in nature, that is, $\mathfrak{L}(x+y) = \mathfrak{L}(x) + \mathfrak{L}(y)$ for all $x, y \in \mathbb{F}_{q^n}$. In fact $\mathfrak{L}(x)$ is a linear transformation from vector space $\mathbb{F}_{q^n}$ to itself with $\mathbb{F}_q$ as field of scalars. The linearized polynomial $\mathfrak{L}(x)$ becomes a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if 0 is the only root of $\mathfrak{L}(x)$ in $\mathbb{F}_{q^n}$. The polynomial $\mathfrak{L}(x) + c$ is said to be an affine polynomial where $c \in \mathbb{F}_{q^n}$ is some constant.

Definition 2.2. [19] Let $\mathbb{F}_{q^n}$ be the extension field of $\mathbb{F}_q$. For any $\gamma \in \mathbb{F}_{q^n}$, Tr$(\gamma)$, the trace of γ over $\mathbb{F}_q$, is a function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ defined as Tr$(\gamma) = \gamma + \gamma^q + \cdots + \gamma^{q^{n-1}}$.

Trace is a linear map (linearized polynomial) from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ and it is a balanced map. This means that it takes exactly q^{n-1} elements of $\mathbb{F}_{q^n}$ to a single element of $\mathbb{F}_q$.

The next lemma provides characterization of linearized polyomial to be a permutation polynomial in general case.

Lemma 2.3. *[19] Let*

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

be a square matrix of order n, where $a_i \in \mathbb{F}_{q^n}, i = 0, 1 \cdots, n-1$. Then the linearized polynomial $\sum_{i=0}^{n-1} a_i x^{q^i}$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if the matrix A is invertible .

Definition 2.4. Suppose p be a prime and m be any positive integer lying in the range $0 \leq m \leq p^{t+1} - 1$. Express m in the power series of base p as $m = \theta_1 + \theta_2 p + \cdots \theta_t p^t$, where $\theta_i \in \{0, 1, \cdots, p-1\}$. The summation $\sum_{i=0}^{t} \theta_i$ is defined as the p-weight of m, usually denoted by $w_p(m)$

Definition 2.5. [23] Let $\phi(x) = c_0 + c_1 x + \cdots + c_t x^t$ be a polynomial over finite field $\mathbb{F}_{p^n}$. Algebraic degree of $\phi(x)$ is defined as the greatest p-weight of any exponent i such that $c_i \neq 0$, that is, algebraic degree of $\phi(x) = max\{w_p(i) : 0 \leq i \leq t$ and $c_i \neq 0\}$.

Example 2.6. The algebraic degree of linearized polynomial $\mathfrak{L}(x)$ is one.

Example 2.7. The algebraic degree of Dembowski-Ostrom polynomial, that is, the algebraic degree of polynomial of the form $\sum_{i,j} a_{ij} x^{p^i+p^j}$ is two.

It is well known that every function ϕ from a finite field $\mathbb{F}_q$ to itself is expressible as a polynomial g over $\mathbb{F}_q$ with deg$(g) \leq q-1$. Therefore every perfect nonlinear function from $\mathbb{F}_q$ to itself is a polynomial over $\mathbb{F}_q$.

Definition 2.8. Let $\phi(x)$ be a polynomial over $\mathbb{F}_q$ and $b \in \mathbb{F}_q^*$. Then the discrete derivative of $\phi(x)$ in the direction of b is defined as

$$\mathfrak{D}(\phi(x)) = \phi(x+b) - \phi(x) - \phi(b).$$

Lemma 2.9. *[9] The discrete derivative of a Dembowski-Ostrom polynomial is a linearized polynomial.*

Proposition 2.10. *Let x^u be a monomial with algebraic degree d over a finite field $\mathbb{F}_{p^n}$. Then its discrete derivative in any direction is a polynomial with algebraic degree $d-1$*

Proof. Let x^u be a monomial with algebraic degree d then u is expressible as $c_1 p^{s_1} + c_2 p^{s_2} + \cdots + c_k p^{s_k}$ with $0 < c_i \leq p-1$ and $\sum_{i=1}^{k} c_i = d$.

$$\begin{aligned}
\mathfrak{D}(x^u) =& (x+a)^u - x^u - a^u \\
=& (x+a)^{\sum_{i=1}^{k} c_i p^{s_i}} - x^u - a^u \\
=& \prod_{i=1}^{k} (x+a)^{c_i p^{s_i}} - x^u - a^u \\
=& \prod_{i=1}^{k} (x^{p^{s_i}} + a^{p^{s_i}})^{c_i} - x^u - a^u \\
=& \prod_{i=1}^{k} \left(x^{c_i p^{s_i}} + \binom{c_i}{1} x^{(c_i-1)p^{s_i}} a^{p^{s_i}} + \cdots \binom{c_i}{c_i} a^{c_i p^{s_i}} \right) - x^u - a^u
\end{aligned}$$

Since $\prod_{i=1}^{k} x^{c_i p^{s_i}} = x^{\sum_{i=1}^{k} c_i p^{s_i}} = x^u$, therefore the maximum p-weight of any exponent in the above product is $d-1$. This proves that the algebraic degree of $\mathfrak{D}(x^u)$ is $d-1$. □

It is easy to see that the discrete derivative is additive in nature, that is, $\mathfrak{D}(\phi(x) + \psi(x)) = \mathfrak{D}(\phi(x)) + \mathfrak{D}(\psi(x))$ and $\mathfrak{D}(a\phi(x)) = a\mathfrak{D}(\phi(x))$ for any polynomials $\phi(x)$ and $\psi(x)$ over $\mathbb{F}_{p^n}$ and for $a \in \mathbb{F}_{p^n}^*$. Therefore for $\phi(x) = \sum \alpha_i x^i$, we have $\mathfrak{D}(\phi(x)) = \sum \alpha_i \mathfrak{D}(x^i)$. In view of this, the following result follows immediately.

Proposition 2.11. *If $\phi(x)$ is any polynomial of algebraic degree d over a finite field $\mathbb{F}_{p^n}$ then its discrete derivative is a polynomial of algebraic degree $d-1$.*

Example 2.12. Consider the polynomial $\phi(x) = x^7$ over $\mathbb{F}_{3^n}$. The algebraic degree of $\phi(x)$ is 3, because $7 = 1{\cdot}3^0 + 2{\cdot}3^1$. The derivative of $\phi(x)$ at any point $a \in \mathbb{F}_{3^n}^*$ is $ax^6 + 2a^3x^4 + 2a^6x^3 + a^6x$. We see that the p-weights of exponents 6, 4, 3, 1 are 2, 2, 1, 1 respectively. Therefore, the algebraic degree of $\phi(x)$ is 2.

3 Families of perfect nonlinear functions over $\mathbb{F}_{p^{2m}}$

In this section, we present two families of perfect nonlinear functions. Like the other known classes, these classes are of Do-type trinomials of the form $Ax^2 + Bx^{p^m+1} + Cx^{p^{2m}}$.

Theorem 3.1. *The function $f_1(x) = -\alpha x^2 + 2\alpha x^{p^m+1} + (\alpha^2+\alpha+1)x^{2p^m}$, where $\alpha \in \mathbb{F}_{p^m}$, and $\alpha \neq \pm 1$, is perfect nonlinear over $\mathbb{F}_{p^n}$ with $n = 2m$.*

Proof. The discrete derivative of $f_1(x)$ at $b \in \mathbb{F}_{p^n}^*$ is $\mathfrak{D}(f_1(x)) = f_1(x+b) - f_1(x) - f_1(b)$. We have, $\mathfrak{D}(f_1(x)) = 2[\{-b\alpha+b^{p^m}\alpha\}x+\{b\alpha+(\alpha^2+\alpha+1)b^{p^m}\}x^{p^m}]$. As we are in the field of odd characteristic, we can ignore the factor 2 in $\mathfrak{D}(f_1(x))$. So, we need to show that the linearized polynomial $\mathfrak{D}(f_1(x)) = \{-b\alpha + b^{p^m}\alpha\}x + \{b\alpha + (\alpha^2+\alpha+1)b^{p^m}\}x^{p^m}$ is invertible. Suppose $x = v$ is a root of $\mathfrak{D}(f_1(x))$. We are done if we show that $v = 0$. We have

$$\mathfrak{D}(f_1(v)) = \{-b\alpha + b^{p^m}\alpha\}v + \{b\alpha + (\alpha^2+\alpha+1)b^{p^m}\}v^{p^m} = 0 \tag{3.1}$$

$$\mathfrak{D}(f_1(v))^{p^m} = \{(\alpha^2+\alpha+1)b + b^{p^m}\alpha\}v + \{b\alpha - b^{p^m}\alpha\}v^{p^m} = 0 \tag{3.2}$$

From $\mathfrak{D}(f_1(v)) - (\mathfrak{D}(f_1(v))^{p^m} = 0$, we obtain $(\alpha+1)^2\{(bv)^{p^m} - bv\} = 0$, yielding

$$(bv)^{p^m} = bv. \tag{3.3}$$

Substituting (3.3) in (3.1) gives

$$(\alpha^2+1)bv + \alpha(b^{p^m}v + bv^{p^m}) = 0$$

or equivalently

$$(\alpha^2+1)bv + \alpha\{\mathrm{Tr}(b)\,\mathrm{Tr}(v) - 2bv\} = 0$$

or

$$(\alpha-1)^2 bv + \alpha\,\mathrm{Tr}(b)\,\mathrm{Tr}(v) = 0. \tag{3.4}$$

Case-1 If $b \in \mathbb{F}_{p^m}^*$, then $(bv)^{p^m} = bv$ implies $v \in \mathbb{F}_{p^m}$ and from (3.4) we find that, $(\alpha+1)^2 bv = 0$ this gives $v = 0$.
Case-2 Suppose $b \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$. Now to show that the linearized polynomial $\mathfrak{D}(f_1(x))$ is invertible, we use *Lemma* 2.3 and show that the determinant $\Delta_1 \neq 0$, where Δ_1 is given by

$$\Delta_1 = \begin{vmatrix} -\alpha b + \alpha b^{p^m} & (\alpha^2+\alpha+1)b + \alpha b^{p^m} \\ \alpha b + (\alpha^2+\alpha+1)b^{p^m} & \alpha b - \alpha b^{p^m} \end{vmatrix}.$$

Solving the determinant, we obtain

$$\Delta_1 = -(\alpha+1)^2 b^2\{(\alpha^2+1)b^{p^m-1} + \alpha(1 + b^{2(p^m-1)})\}. \tag{3.5}$$

We claim that either $b^{p^m-1} = -1$ or $b^{p^m-1} \in \mathbb{F}_{p^{2m}} \backslash \mathbb{F}_{p^m}$. If $b^{p^m-1} \in \mathbb{F}_{p^m}^*$, then $(b^{p^m-1})^{p^m-1} = 1$. This implies $b^{2(p^m-1)} = 1$ and therefore $b^{p^m-1} = -1$. Hence, it follows that either $b^{p^m-1} = -1$ or $b^{p^m-1} \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$. For convenience let us denote b^{p^m-1} by β and simplifying (3.5) we get

$$-\Delta_1 = (\alpha+1)^2 b^2(\alpha+\beta)(\alpha\beta+1). \tag{3.6}$$

If $\beta = -1$, we see that $-\Delta_1 = (\alpha+1)^2 b^2(\alpha-1)(1-\alpha) \neq 0$.

Next, if $\beta \neq -1$, then $\beta \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ and $\alpha \in \mathbb{F}_{p^m}$ therefore, $\alpha+\beta \neq 0$ and $\alpha\beta \neq -1$. From (3.6) it follows that $\Delta_1 \neq 0$. □

Theorem 3.2. *The function*

$$f_2(x) = -\alpha(\alpha+1)x^2 + 2\alpha(\alpha+1)x^{p^m+1} + (3\alpha^2+3\alpha+1)x^{2p^m}$$

is perfect nonlinear over $\mathbb{F}_{p^n}$ *with* $n = 2m$ *and* $\alpha \in \mathbb{F}_{p^m}, 2\alpha+1 \neq 0$.

Proof. $f_2(x) = -\alpha(\alpha+1)x^2 + 2\alpha(\alpha+1)x^{p^m+1} + (3\alpha^2+3\alpha+1)x^{2p^m}$. Its discrete derivative $\mathfrak{D}(f_2(x)) = \{-\alpha(1+\alpha)b+\alpha(1+\alpha)b^{p^m}\}x+\{\alpha(1+\alpha)b+(3\alpha^2+3\alpha+1)b^{p^m}\}x^{p^m}$ is a linearized polynomial over $\mathbb{F}_{p^n}$. Let v be a root of $\mathfrak{D}(f_2(x))$. We have

$$\mathfrak{D}(f_2(v)) = \{\alpha(1+\alpha)(-b+b^{p^m})\}v + \{\alpha(1+\alpha)b + (3\alpha^2+3\alpha+1)b^{p^m}\}v^{p^m} \tag{3.7}$$

and

$$\mathfrak{D}(f_2(v))^{p^m} = \{(3\alpha^2+3\alpha+1)b + \alpha(1+\alpha)b^{p^m}\}v + \{\alpha(1+\alpha)(b-b^{p^m})\}v^{p^m}. \tag{3.8}$$

Since $\mathfrak{D}(f_2(v)) = 0$, we have $\mathfrak{D}(f_2(v)) - \mathfrak{D}(f_2(v))^{p^m} = 0$. This gives $(2\alpha+1)^2bv - (2\alpha+1)^2(bv)^{p^m} = 0$
or equivalently, we have

$$(bv)^{p^m} = bv. \tag{3.9}$$

Substituting (3.9) in (3.7) gives

$$(2\alpha^2+2\alpha+1)bv + \alpha(\alpha+1)\{b^{p^m}v + bv^{p^m}\} = 0$$

which is furhter equivalent to

$$(2\alpha^2+2\alpha+1)bv + \alpha(\alpha+1)\{\mathrm{Tr}(b)\,\mathrm{Tr}(v) - 2bv\} = 0$$

or

$$bv + \alpha(\alpha+1)\ \mathrm{Tr}(b)\,\mathrm{Tr}(v) = 0. \tag{3.10}$$

Case-1 If $b \in \mathbb{F}_{p^m}^*$, then $(bv)^{p^m} = bv$ implies that $v \in \mathbb{F}_{p^m}$ and from (3.10) it follows that $(2\alpha+1)^2bv = 0$ and this gives $v = 0$.
Case-2 Now assume $b \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$. We show that the determinant $\Delta_2 \neq 0$, where Δ_2 is given by

$$\Delta_2 = \begin{vmatrix} \alpha(\alpha+1)(b^{p^m}-b) & (3\alpha^2+3\alpha+1)b + \alpha(\alpha+1)b^{p^m} \\ \alpha(\alpha+1)b + (3\alpha^2+3\alpha+1)b^{p^m} & \alpha(\alpha+1)(b-b^{p^m}) \end{vmatrix}.$$

Solving the determinant we have

$$\begin{aligned} \Delta_2 &= -\,(2\alpha+1)^2\{\alpha(\alpha+1)(b^2+b^{2p^m}) + (2\alpha^2+2\alpha+1)b^{p^m+1}\} \\ &= -\,(2\alpha+1)^2b^2\{\alpha(\alpha+1)(1+b^{p^m-1})^2 + b^{p^m-1}\} \end{aligned}$$

Following a similar argument as in $Theorem$ 3.1, it follows that $b^{p^m-1} \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ or $b^{p^m-1} = -1$ and we identify b^{p^m-1} by β.

$$\begin{aligned} \Delta_2 &= -(2\alpha+1)^2b^2\{\alpha(\alpha+1)(1+\beta)^2 + \beta\} \\ &= -(2\alpha+1)^2b^2(\beta(1+\alpha)+\alpha)(\alpha\beta+\alpha+1) \end{aligned}$$

If $\beta = -1$, then $\Delta_2 = (2\alpha+1)^2b^2 \neq 0$. Next, if $\beta \neq -1$, then $\beta \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ and $\alpha \in \mathbb{F}_{p^m}$. This gives, $\alpha+\beta, \alpha\beta \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$. Consequently, we have $\beta(1+\alpha)+\alpha \neq 0$ and $\alpha\beta+\alpha+1 \neq 0$, and this concludes that $\Delta_2 \neq 0$. □

4 Perfect Nonlinear functions over $\mathbb{F}_{p^{3m}}$

In this section, we propose two classes of planar functions over finite fields $\mathbb{F}_{p^{3m}}$.

Theorem 4.1. *The function* $f_3(x) = -\alpha x^2 - 2x^{p^m+1} + 2(\alpha+1)x^{p^{2m}+1} - \alpha x^{2p^m} + 2(\alpha+1)x^{p^{2m}+p^m} + (\alpha^2+2\alpha+2)x^{2p^{2m}}$ *is a perfect nonlinear function over* $\mathbb{F}_{p^n}$ *where* $\alpha \in \mathbb{F}_{p^m}$*,* $\alpha \neq 1, -2$ *and* $n = 3m$*.*

Proof. For $f_3(x) = -\alpha x^2 - 2x^{p^m+1} + 2(\alpha+1)x^{p^{2m}+1} - \alpha x^{2p^m} + 2(\alpha+1)x^{p^{2m}+p^m} + (\alpha^2 + 2\alpha+2)x^{2p^{2m}}$, its discrete derivative at any $b \in \mathbb{F}_{p^n}^*$ is

$$\begin{aligned}
\mathfrak{D}(f_3(x)) &= f_3(x+b) - f_3(x) - f_3(b)\\
&= \{-\alpha b - b^{p^m} + (\alpha+1)b^{p^{2m}}\}x + \{-b - \alpha b^{p^m} + (\alpha+1)b^{p^{2m}}\}x^{p^m}\\
&+ \{(\alpha+1)(b + b^{p^m}) + (\alpha^2+2\alpha+2)b^{p^{2m}}\}x^{p^{2m}}\\
\mathfrak{D}(f_3(x))^{p^m} &= \{(\alpha^2+2\alpha+2)b + (1+\alpha)(b^{p^m} + b^{p^{2m}})\}x\\
&+ \{(1+\alpha)b - \alpha b^{p^m} - b^{p^{2m}}\}x^{p^m}\\
&+ \{(1+\alpha)b - b^{p^m} - \alpha b^{p^{2m}}\}x^{p^{2m}}\\
\mathfrak{D}(f_3(x))^{p^{2m}} &= \{-\alpha b + (1+\alpha)b^{p^m} - b^{p^{2m}}\}x\\
&+ \{(1+\alpha)b + (\alpha^2+2\alpha+2)b^{p^m} + (1+\alpha)b^{p^{2m}}\}x^{p^m}\\
&+ \{-b + (1+\alpha)b^{p^m} - \alpha b^{p^{2m}}\}x^{p^{2m}}
\end{aligned}$$

Let v be a root of $\mathfrak{D}(f_3(x))$. Then we have

$$\begin{aligned}
\mathfrak{D}(f_3(v)) = \{-\alpha b - b^{p^m} + (\alpha+1)b^{p^{2m}}\}v + \{-b - \alpha b^{p^m} + (\alpha+1)b^{p^{2m}}\}v^{p^m}\\
+ \{(\alpha+1)(b + b^{p^m}) + (\alpha^2+2\alpha+2)b^{p^{2m}}\}v^{p^{2m}} = 0
\end{aligned}$$

and $\mathbb{D}(v) = \mathfrak{D}(f_3(v)) + \alpha\mathfrak{D}(f_3(v))^{p^m} + \mathfrak{D}(f_3(v))^{p^{2m}} = 0$. We have

$$\begin{aligned}
\mathbb{D}(v) &= \alpha(\alpha+2)\{\alpha b + b^{p^m} + b^{p^{2m}}\}v + (\alpha+2)\{\alpha b + b^{p^m} + b^{p^{2m}}\}v^{p^m}\\
&+ (\alpha+2)\{\alpha b + b^{p^m} + b^{p^{2m}}\}v^{p^{2m}}\\
&= (\alpha+2)\{\alpha b + b^{p^m} + b^{p^{2m}}\}\{\alpha v + v^{p^m} + v^{p^{2m}}\}.
\end{aligned}$$

Assuming $L(x) = \alpha x + x^{p^m} + x^{p^{2m}}$, we have $\mathbb{D}(v) = (\alpha+2)L(b)L(v)$. Moreover, we find that

$$\begin{vmatrix} \alpha & 1 & 1\\ 1 & \alpha & 1\\ 1 & 1 & \alpha \end{vmatrix} = (\alpha-1)^2(\alpha+2) \neq 0.$$

In view of *Lemma* 2.3 it is evident that the linearized polynomial $L(x)$ is invertible and hence $L(b) \neq 0$. Therefore, $\mathfrak{D}(f_3(v)) = 0$ implies $v = 0$. □

Theorem 4.2. *The polynomial* $f_4(x) = u^3x^2 + 2u^2x^{p^m+1} + (u^2+u)x^{2p^m} + 2ux^{p^{2m}+p^m} + x^{2p^{2m}}$ *is a planar function over* $\mathbb{F}_{p^n}$ *with* $n = 3m$ *if* $u^3 + 1 \neq 0$.

Proof. Let $\mathfrak{D}(f_4(x)) = f_4(x+b) - f_4(x) - f_4(b)$ for any $b \in \mathbb{F}_{p^{3m}}^*$. A simple calculation gives,

$$\mathfrak{D}(f_4(x)) = 2\{(u^3b + u^2b^{p^m})x + (u^2b + u^2b^{p^m} + ub^{p^m} + ub^{p^{2m}})x^{p^m} + (ub^{p^m} + b^{p^{2m}})x^{p^{2m}}\}$$

$f_4(x)$ is planar if and only if $\mathfrak{D}(f_4(x))$ is a premutation polynomial of $\mathbb{F}_{p^{3m}}$. Since $2 \neq p$, without loss of generality, we may ignore the factor 2 in $\mathfrak{D}(f_4(x))$.

Taking p^m-th and p^{2m}-th power of $\mathfrak{D}(f_4(x))$ we have,

$$\mathfrak{D}(f_4(x))^{p^m} = (b^{p^m}+ub^{p^{2m}})x+(u^3b^{p^m}+u^2b^{p^{2m}})x^{p^m}+(u^2b^{p^m}+u^2b^{p^{2m}}+ub^{p^{2m}}+ub)x^{p^{2m}} \tag{4.1}$$

and

$$\mathfrak{D}(f_4(x))^{p^{2m}} = (u^2b^{p^{2m}} + u^2b + ub + ub^{p^m})x + (b^{p^{2m}} + ub)x^{p^m} + (u^3b^{p^{2m}} + u^2b)x^{p^{2m}} \tag{4.2}$$

The polynomial $\mathfrak{D}(f_4(x))$ is a linearized polynomial. Suppose α be any zero of $\mathfrak{D}(f_4(x))$. It suffices to show that $\alpha = 0$. If possible suppose $\alpha \neq 0$.

Consider the polynomial $S(x) = \mathfrak{D}(f_4(x)) + u^2\mathfrak{D}(f_4(x))^{p^m} - u\mathfrak{D}(f_4(x))^{p^{2m}}$. We have,

$$\begin{aligned} S(x) =&(u^2b^{p^m} + ub^{p^{2m}} + u^5b^{p^m} + u^4b^{p^{2m}})x^{p^m} + (ub^{p^m} + b^{p^{2m}} + u^4b^{p^m} + u^3b^{p^{2m}})x^{p^{2m}} \\ =&u(u^3+1)(ub^{p^m} + b^{p^{2m}})x^{p^m} + (u^3+1)(ub^{p^m} + b^{p^{2m}})x^{p^{2m}} \\ =&(u^3+1)(ub^{p^m} + b^{p^{2m}})(ux^{p^m} + x^{p^{2m}}) \end{aligned}$$

Consider the linearized polynomial $H(x) = (ux^{p^m} + x^{p^{2m}})$ over $\mathbb{F}_{p^{3m}}$. We see that

$$\begin{vmatrix} 0 & 1 & u \\ u & 0 & 1 \\ 1 & u & 0 \end{vmatrix} = u^3 + 1 \neq 0$$

From $Lemma$ 2.3, it follows that $H(x)$ is a permutation polynomial and consequently $S(x) \neq 0$ for all $x \in \mathbb{F}^*_{p^{3m}}$. However, we have $\alpha \in \mathbb{F}^*_{p^{3m}}$ such that $\mathfrak{D}(f_4(\alpha)) = 0$. This implies that $S(\alpha) = 0$ and we arrive at contradiction.

□

5 Conclusion

In this article, we have obtained four classes of perfect nonlinear functions over finite fields of arbitrary odd characteristic. Our classes, like other known classes, are DO-type polynomials. Since the paper's main aim is to propose four classes of perfect nonlinear functions, we have refrained from studying their semifields and their inequivalence with the known families of perfect nonlinear functions. It needs further investigation in this direction.

References

[1] Y. Akbal, B. G. Temür, P. Ongan, *A short note on permutation trinomials of prescribed type*, Comm. Algebra, **48(4)** (2020), 1608-1612

[2] D. Bartoli, M. Bonini, *Planar Polynomials arising from Linearized polynomials*, J. Algebra Appl., **21(01)** 2022, 2250002(1-8).

[3] G. R. V. Bhatta, B. Shankar, V. N. Mishra, P. Poojary *Sequences of numbers via permutation polynomials over some finite rings*, Proyecciones, **39** (2020) 1295–1313.

[4] L. Budaghyan, T. Helleseth, *New commutative semifields defined by new PN multinomials*, Cryptogr. Commun. **3** (2011), 1–16.

[5] C. Blondean, K. Nyberg, *Perfect nonlinear functions and Cryptography*, Finite Fields App., **32** (2015), 120-147.

[6] 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.

[7] R. S. Coulter, *On the classification of planar monomials over fields of square order*, Finite Fields Appl., **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] R. Gupta, R. K. Sharma, *Further results on permutation polynomials of the form $(x^{p^m} - x + \delta)s + x$ over $\mathbb{F}_{p^{2m}}$*, Finite Fields Appl., **50** (2018) 196-208.

[11] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory*, Finite Fields Appl., **13** (2007), 58-70.

[12] Y. Laigle-Chapuy, *A Note on a Class of Quadratic Permutations over $\mathbb{F}_{2^n}$, In Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* AAECC 2007 (Springer, Berlin, 2007), 130-137.

[13] P. Dembowski, T. G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Zeit., **103** (1968), 239-258.

[14] C. Ding, J. Yuan *A family of skew Hadamard difference sets*, J. Comb. Theory, Ser. A, **113** (2006), 1526-1535.

[15] N. Fernando, *A note on permutation binomials and trinomials over finite fields*, New Zeland J. Math., **48**(2018) 25-29.

[16] X. Gong, G. Gao, W. Liu, *On permutation polynomials of the form* $x^{1+2^k} + L(x)$ Int. J. Comput. Math., **93(10)** (2016), 1715-1722.

[17] V. Jarali , P. Poojary, VGR Bhatta, *Construction of Permutation Polynomials Using Additive and Multiplicative Characters*, Symmetry, **14(8)** (2022), 1539.

[18] C. Li, T. Helleseth, *Quasi-perfect linear codes from planar and APN functions*, Cryptogr. Commun., **8** (2016), 215–227.

[19] R. Lidl , H. Niederreiter, *Finite Fields, Encyclopaedia of mathematics and its Applications*, Cambridge University Press, 2003.

[20] G. L. Mullen, D. Panario, *Handbook of Finite Fields*, CRC Press, Taylor & Francis Group, 2013.

[21] P. Ongan, B. G. Temür, *Some permutations and complete permutation polynomials over finite fields*, Turkish J. Math., **43(5)** (2019), 2154-2160.

[22] P. Ongan, B. G. Temür, *A specific type of permutation and complete permutation polynomials over finite fields*, J. Algebra its Appl., **19(04)** (2020), 2050067.

[23] A. Pott, *Almost perfect and planar functions*, Des. Codes Cryptogr., **78** (2016), 141-195.

[24] R. P. Singh, A. Saikia, B. K. Sarma, *Poly-dragon: an efficient multivariate public key cryptosystem* J. Math. Cryptol., **4(4)** (2011), 349-364.

[25] 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.

[26] R. P. Singh, M. K. Singh, *Two congurence identities on ordered partitions*, INTEGERS: Electronic journal of Combinatorial Number Theory, **18** (2018), A73.

Author information

Dhananjay Kumar, Department of Mathematics, National Institute of Technology Patna, India.
E-mail: dhananjay.ma17@nitp.ac.in

Rajesh P. Singh, Department of Mathematics, Central University of South Bihar, India.
E-mail: rpsingh@cub.ac.in (Corresponding Author)

Rishi Kumar Jha, Department of Mathematics, National Institute of Technology Patna, India.
E-mail: rkjha@nitp.ac.in