Süleyman Demirel Üniversitesi Fen Edebiyat Fakültesi Fen Dergisi
Süleyman Demirel University Faculty of Arts and Sciences Journal of Science
2022, 17(2): 261-269
DOI: 10.29233/sdufeffd.1053097
Atıf için / For Citation: Z. Aksoy, B. B. Kırlar, "On the planarity of certain Dembowski-Ostrom polynomials", *Süleyman Demirel Üniversitesi Fen Edebiyat Fakültesi Fen Dergisi*, 17(2), 261-269, 2022.

Research Article

On the Planarity of Certain Dembowski-Ostrom Polynomials

Zehra AKSOY[1], Barış Bülent KIRLAR[*2]

[1]*Süleyman Demirel University, Graduate School of Natural and Applied Sciences, Department of Mathematics, 32260, Isparta, Turkey*
[2]*Süleyman Demirel University, Faculty of Arts and Sciences, Department of Mathematics, 32260, Isparta, Turkey*

**corresponding author e-mail: bariskirlar@sdu.edu.tr*

(Alınış / Received: 03.01.2022, Kabul / Accepted: 23.06.2022, Yayımlanma / Published: 25.11.2022)

Abstract: Planar mappings, defined by Dembowski and Ostrom, are identified as a means to construct projective planes. Then, many important applications of planar mappings appear in different fields such as cryptography and coding theory. In this paper, we provide sufficient and necessary conditions for the planarity of certain Dembowski-Ostrom polynomials over the finite field extension of degree three with odd characteristic. In particular, we completely determine the coefficients of the given Dembowski-Ostrom polynomials to be planar.

***Key words**:* Linearized polynomials, Dembowski-Ostrom polynomials, Planar mappings

Bazı Dembowski-Ostrom Polinomlarının Planaritesi Üzerine

Öz: Dembowski ve Ostrom tarafından tanımlanan planar dönüşümler projektif düzlemler oluşturmanın bir yolu olarak ortaya çıkmıştır. Sonrasında, planar dönüşümlerin kriptografi ve kodlama teorisi gibi farklı alanlarda birçok önemli uygulaması yapılmıştır. Bu çalışmada, tek karakteristiğe sahip üçüncü dereceden sonlu cisim genişlemeleri üzerinde tanımlanan belirli bir formdaki Dembowski-Ostrom polinomlarının planaritesi için gerek ve yeter koşullar elde edilmiştir. Özel olarak, verilen Dembowski-Ostrom polinomlarının planar olmasını sağlayan katsayılar tamamıyla belirlenmiştir.

***Anahtar kelimeler**:* Lineerize polinomlar, Dembowski-Ostrom polinomları, Planar dönüşümler

Zehra AKSOY, zhraaksoy@gmail.com, ORCID: https://orcid.org/0000-0003-4534-3958
Barış Bülent KIRLAR, bariskirlar@sdu.edu.tr, ORCID: https://orcid.org/0000-0003-0112-1974

1. Introduction and Preliminaries

Let F_{q^n} be a finite field of characteristic p, then a linearized polynomial over F_{q^n}, which is also so-called q-polynomial over F_{q^n}, is defined by

$$L:\mathrm{F}_{q^n} \to \mathrm{F}_{q^n}$$

$$x \mapsto L(x) = \sum_{i=0}^{n} a_i x^{q^i}$$

with coefficients $a_i \in \mathrm{F}_q$. These polynomials have been investigated by Ore [19, 20]. A linearized polynomial particularly defines a bijective mapping if and only if its root is only $x = 0$. On the other hand, a well-known result of Dickson shows that a linearized polynomial $L(x) = \sum_{i=0}^{n} a_i x^{q^i} \in \mathrm{F}_{q^n}$ describes a permutation polynomial if and only if the Dickson matrix

$$\mathrm{D_L} = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1}^q & a_0^q & \dots & a_{n-2}^q \\ \vdots & \vdots & & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \dots & a_0^{q^{n-1}} \end{pmatrix}$$

is non-singular [15]. It means that a permutation polynomial is just a linearized polynomial of rank n. Linearized polynomials have also plenty applications in cryptography and coding theory [2, 12, 21, 25].

Note that a mapping is called quadratic if it is represented by a polynomial with algebraic degree 2. The following important class of polynomials with algebraic degree 2 defined over F_{q^n}

$$\sum_{\substack{i,j=0,\dots,n-1 \\ i \le j}} a_{i,j} x^{q^i+q^j}$$

is so-called Dembowski-Ostrom polynomials [6]. These polynomials, defined by Dembowski and Ostrom, have an importance in the study of specific projective planes. They construct many translation planes and finite commutative semifields which are the subjects of finite geometry [6,8]. For more information about these polynomials, please see [5,6,7,27].

Let q be a power of odd prime p. Then,

$$D_{f,\alpha}:\mathrm{F}_{q^n} \to \mathrm{F}_{q^n}$$

$$x \mapsto f(x+\alpha) - f(x) - f(\alpha)$$

is called difference mapping of f defined by α for $f:\mathrm{F}_{q^n} \to \mathrm{F}_{q^n}$ and $\alpha \in \mathrm{F}_{q^n}^* = \mathrm{F}_{q^n} \setminus \{0\}$. In [6], Dembowski-Ostrom polynomials have been characterized by difference mappings. According to this characterization, a polynomial f is Dembowski-Ostrom

polynomial if and only if all difference mappings are linearized polynomial for each $\alpha \in \mathrm{F}_{q^n}^*$. Moreover, a mapping $f : \mathrm{F}_{q^n} \to \mathrm{F}_{q^n}$ is called planar if its all difference mappings are bijective.

Planar mappings, defined by Dembowski and Ostrom, have been identified as a means to construct projective planes [7]. In cryptography, planar mappings are called perfect nonlinear (PN) functions and they supply the best resistance to differential attack when used as an S-box in block ciphers [17,18]. Perfect nonlinear functions, defined by Meier and Staffelbach [16], have been used to construct as authentication codes [9], optimal constant-composition codes [11], secret sharing schemes resulting from particular linear codes [4] and signal sets [10]. Perfect nonlinear functions have been also used to construct DES-like cryptosystems. Planar mappings are not available over finite fields of even characteristic since if x is a solution for difference mappings so is $x+\alpha$. In recent times, Zhou [28] introduces a native analogue of planar mappings over finite fields of even characteristic which has similar manner for planar functions over finite fields of odd characteristic [24,28]. He showed that a function $f : \mathrm{F}_{2^n} \to \mathrm{F}_{2^n}$ is called planar if the map $x \mapsto f(x+\alpha)+f(x)+\alpha x$ is bijective for each $\alpha \in \mathrm{F}_{2^n}^*$. Dembowski and Ostrom claim that every planar mapping over F_{q^n} is necessarily a Dembowski-Ostrom polynomial. This is rearticulated as a conjecture in [22]. Coulter and Matthews [6] and Singh [26] describe new classes of planar polynomials which provide counter examples to this conjecture in F_{3^n} and in F_{p^n} with $p \geq 3$, respectively.

A polynomial that can be written as a product of two linearized polynomials $L_1(x)$ and $L_2(x)$ is called bilinear polynomial [23], otherwise it can be so-called non-bilinear. If $q \neq 2$, all bilinear polynomials over F_{q^n} are Dembowski-Ostrom polynomials [3]. If $q = 2$, bilinear polynomial $P(x)$ defines Dembowski-Ostrom polynomial over F_{2^n} for linearized polynomials except that $L_1 = L_2$. However, every Dembowski-Ostrom polynomial does not have to be the bilinear polynomial. For example, $f(x) = x^{10} + x^6 - x^2$ over F_{3^e} is a non-bilinear Dembowski-Ostrom polynomial which is planar if and only if $e = 2$ or e is odd [6]. Also, $f(x) = x^{(3\alpha+1)/2}$ over F_{3^e}, which is not a bilinear Dembowski-Ostrom polynomial, is planar if and only if $\gcd(\alpha, e) = 1$ and α is odd [6]. Kyureghyan and Özbudak investigate the planarity of bilinear Dembowski-Ostrom polynomials in the form $L_1(x) \cdot L_2(x)$ over F_{q^n}, which are extended affine equivalent (EA-equivalent) to $x \cdot L(x)$ [13]. In particular, they show under what condition certain forms of Dembowski-Ostrom polynomials over F_{q^2} and F_{q^3} are planar. Then, Kyureghyan, Özbudak and Pott completely classify q-quadratic planar binomials over F_{q^3} using the related algebraic function fields [14]. In recent times, Bartoli and Bonini provide planar polynomials of the form $f_{A,B}(x) = x(x^{q^2} + Ax^q + Bx)$ over F_{q^3}, where $A, B \in \mathrm{F}_q$, by utilizing the connections with algebraic curves over finite fields [1].

1.1 Our contribution

In this paper, we suggest the planarity of Dembowski-Ostrom polynomials over F_{q^3} with odd characteristic of the form

$$f(x) = x^{2q^2} + x^{2q} + x^2 + Ax^{q+1} + Bx^{q^2+1} + Cx^{q^2+q}, \qquad A, B, C \in \mathrm{F}_q,$$

which cannot be written as a product of two linearized polynomials. Therefore, this type of polynomials can be so-called non-bilinear Dembowski-Ostrom polynomials. In particular, we completely determine the triples $(A, B, C) \in \mathrm{F}_q^3$ such that $f(x)$ is planar by applying connections with algebraic curves over finite fields, inspiring the work in [1]. This was also carried out by combining some q-quadratic binomials over F_{q^3} used in [14].

1.2 Outline

The remainder of the paper is structured as follows. In Section 2 we first introduce a certain class of non-bilinear Dembowski-Ostrom polynomials. Based on the fact that all difference mappings must be bijective for a polynomial to define planar mappings, and that the difference mappings of Dembowski-Ostrom polynomials are linearized polynomials, we use the Dickson matrices that allow us to learn whether linear polynomials are permutation polynomials. Then, using the relationship between the determinant polynomial obtained from Dickson matrix and the algebraic curves defined over finite fields, we state sufficient and necessary conditions for the planarity of our polynomial class. We conclude the paper in Section 3.

2. Main Results

Let

$$f(x) = x^{2q^2} + x^{2q} + x^2 + Ax^{q+1} + Bx^{q^2+1} + Cx^{q^2+q} \tag{1}$$

be a polynomial over F_{q^3} with odd characteristic, where $A, B, C \in \mathrm{F}_q$. Eq. (1) can also be expressed as follows:

$$f(x) = Tr(x^2) + x(Ax^q + Bx^{q^2} + Cx^{q^2+q-1}),$$

where Tr is the trace function from F_{q^3} to F_q. It is easy to see that Eq. (1) cannot be written as a product of two linearized polynomials. Therefore, it defines a non-bilinear Dembowski-Ostrom polynomial. Eq. (1) is planar if and only if for each $\alpha \in \mathrm{F}_{q^3}^*$, the difference mapping

$$\begin{aligned} D_{f,\alpha}(x) &= f(x+\alpha) - f(x) - f(\alpha) \\ &= (2\alpha^{q^2} + C\alpha^q + B\alpha)x^{q^2} + (C\alpha^{q^2} + 2\alpha^q + A\alpha)x^q + (B\alpha^{q^2} + A\alpha^q + 2\alpha)x \end{aligned}$$

is a permutation polynomial. $D_{f,\alpha}$ is a permutation polynomial if and only if the Dickson matrix

$$\mathrm{D_L} = \begin{pmatrix} B\alpha^{q^2} + A\alpha^q + 2\alpha & C\alpha^{q^2} + 2\alpha^q + A\alpha & 2\alpha^{q^2} + C\alpha^q + B\alpha \\ 2\alpha + C\alpha^{q^2} + B\alpha^q & B\alpha + A\alpha^{q^2} + 2\alpha^q & C\alpha + 2\alpha^{q^2} + A\alpha^q \\ C\alpha^q + 2\alpha + A\alpha^{q^2} & 2\alpha^q + C\alpha + B\alpha^{q^2} & B\alpha^q + A\alpha + 2\alpha^{q^2} \end{pmatrix}$$

is non-singular. We obtain the determinant polynomial from the Dickson matrix $\mathrm{D_L}$ as follows:

$$G(\alpha, \alpha^q, \alpha^{q^2}) = \alpha^{q^2+q+1}(2A^3 + 2B^3 + 2C^3 - 6ABC)$$
$$+(\alpha^{2q^2+q} + \alpha^{2q^2+1} + \alpha^{q^2+2q} + \alpha^{q^2+2} + \alpha^{2q+1} + \alpha^{q+2})(2A^2 + 2B^2 + 2C^2 - 2AB - 2AC - 2BC)$$

$$+(\alpha^3 + \alpha^{3q} + \alpha^{3q^2})(-2A^2 - 2B^2 - 2C^2 + 2AB + 2AC + 2BC). \quad (2)$$

We rewrite Eq. (2) using the affine coordinates $\alpha = X$, $\alpha^q = Y$ and $\alpha^{q^2} = 1$ to find the affine form. Consequently, we get

$$\begin{aligned} F(X,Y) &= -2(A^2 + B^2 + C^2 - AB - AC - BC)(X^3 + Y^3 + 1) \\ &\quad +2(A^2 + B^2 + C^2 - AB - AC - BC)(X^2 + Y^2 + X^2Y + Y^2X + X + Y) \\ &\quad +2(A^3 + B^3 + C^3 - 3ABC)(XY), \end{aligned} \quad (3)$$

that is associated with difference mappings $D_{f,\alpha}$ of Eq. (1).

Lemma 1. Let C be a cubic curve defined by

$$\begin{aligned} F(X,Y) &= -2(A^2 + B^2 + C^2 - AB - AC - BC)(X^3 + Y^3 + 1) \\ &\quad +2(A^2 + B^2 + C^2 - AB - AC - BC)(X^2 + Y^2 + X^2Y + Y^2X + X + Y) \\ &\quad +2(A^3 + B^3 + C^3 - 3ABC)(XY) = 0, \end{aligned}$$

where $A, B, C \in \mathrm{F}_q$. If the cubic curve C has a factor of the form $Y - aX - b$ with $ab \neq 0$, then either of the followings holds

(i) $A^3 + B^3 + C^3 - 3ABC = -2(A^2 + B^2 + C^2 - AB - AC - BC)$,

(ii) $A^3 + B^3 + C^3 - 3ABC = 6(A^2 + B^2 + C^2 - AB - AC - BC)$.

Proof. If a cubic curve is reducible, it has at least a line as a factor. We assume that the cubic curve C has a factor of the form $Y - aX - b$ with $ab \neq 0$. Then, it must satisfy the following condition

$$F(X, aX + b) = 0. \quad (4)$$

By direct computations, Eq. (4) is satisfied if and only if the following equations are provided:

$$-2(a-1)^2(a+1)(A^2 + B^2 + C^2 - AB - AC - BC) = 0, \quad (5)$$

$$-2(b-1)^2(b+1)(A^2 + B^2 + C^2 - AB - AC - BC) = 0, \quad (6)$$

$$2a(A^3+B^3+C^3-3ABC)+$$
$$(2a^2+2+4ab+2b-6a^2b)(A^2+B^2+C^2-AB-AC-BC)=0, \tag{7}$$

$$2b(A^3+B^3+C^3-3ABC)+$$
$$(2b^2+2+4ab+2a-6ab^2)(A^2+B^2+C^2-AB-AC-BC)=0. \tag{8}$$

We now examine the above equations in three cases considering the roots of Eq. (5):

1) $a=1$.

- If $b=1$ or $b=-1$, then using Eq. (7) and Eq. (8) we obtain

$$A^3+B^3+C^3-3ABC=-2(A^2+B^2+C^2-AB-AC-BC) \tag{9}$$

- If $A^2+B^2+C^2-AB-AC-BC=0$, we have

$$A^3+B^3+C^3-3ABC=0$$

from Eq. (7) and

$$b(A^3+B^3+C^3-3ABC)=0$$

from Eq. (8).

2) $a=-1$.

- If $b=1$, then using Eq. (7) and Eq. (8) we obtain

$$A^3+B^3+C^3-3ABC=-2(A^2+B^2+C^2-AB-AC-BC)$$

- If $b=-1$, then using Eq. (7) and Eq. (8) we obtain

$$A^3+B^3+C^3-3ABC=6(A^2+B^2+C^2-AB-AC-BC) \tag{10}$$

- If $A^2+B^2+C^2-AB-AC-BC=0$, we have

$$A^3+B^3+C^3-3ABC=0$$

from Eq. (7) and

$$b(A^3+B^3+C^3-3ABC)=0$$

from Eq. (8).

3) $A^2+B^2+C^2-AB-AC-BC=0$.

- $$a(A^3+B^3+C^3-3ABC)=0$$

from Eq. (7) and

$$b(A^3+B^3+C^3-3ABC)=0$$

from Eq. (8). Since $ab \neq 0$, we obtain

$$A^3 + B^3 + C^3 - 3ABC = 0 \tag{11}$$

If we insert Eq. (9) into Eq. (3) and Eq. (10) into Eq. (3) respectively, we obtain the reduced polynomials

$$F(X,Y) = -2(A^2 + B^2 + C^2 - AB - AC - BC)(Y - X - 1)(Y - X + 1)(Y + X - 1)$$

and

$$F(X,Y) = 2(A^2 + B^2 + C^2 - AB - AC - BC)(Y + X + 1)(-X^2 - Y^2 + 2X + 2Y + 2XY - 1).$$

If we insert Eq. (11) into Eq. (3), we have the polynomial

$$F(X,Y) = 2(A^2 + B^2 + C^2 - AB - AC - BC)(-X^3 - Y^3 + X^2 + Y^2 + X^2Y + Y^2X + X + Y - 1),$$

which is irreducible. Therefore, this situation is ignored so as not have a factor of the form $Y - aX - b$.

In the following main theorem, we reduce the problem of finding planarity of polynomial $f(x)$ to the problem of reducibility of cubic curve.

Theorem 2. Let q be a power of odd prime p and consider the polynomial $f(x) \in \mathrm{F}_{q^3}[x]$ of the form

$$f(x) = x^{2q^2} + x^{2q} + x^2 + Ax^{q+1} + Bx^{q^2+1} + Cx^{q^2+q},$$

where $A, B, C \in \mathrm{F}_q$ and $A^2 + B^2 + C^2 - AB - AC - BC \neq 0$. Then, $f(x)$ is planar if and only if either of the followings holds

(i) $A^3 + B^3 + C^3 - 3ABC \neq -2(A^2 + B^2 + C^2 - AB - AC - BC)$,

(ii) $A^3 + B^3 + C^3 - 3ABC \neq 6(A^2 + B^2 + C^2 - AB - AC - BC)$.

Proof. Eq. (1) is planar if and only if $\det(\mathrm{D_L}) \neq 0$. This is analogous to the determinant polynomial $G(\alpha, \alpha^q, \alpha^{q^2})$ of the Dickson matrix $\mathrm{D_L}$, which is not zero. By applying the homogenization to Eq. (2), we obtain the cubic polynomial in Eq. (3). $G(\alpha, \alpha^q, \alpha^{q^2}) \neq 0$ corresponds to circumstances in which the cubic polynomial is irreducible. To find these cases, we need to determine and rule out those that are reducible. If a cubic curve is reducible, it must have at least one line as a factor. In Lemma 1, assuming that the cubic curve has a factor in the type $Y - aX - b$, we find the following cases

$$A^3 + B^3 + C^3 - 3ABC = -2(A^2 + B^2 + C^2 - AB - AC - BC)$$

and

$$A^3 + B^3 + C^3 - 3ABC = 6(A^2 + B^2 + C^2 - AB - AC - BC),$$

where the cubic curve is reducible, and so the planarity is disappeared. On the other hand, the cubic polynomial is irreducible in the case of Eq. (11). Therefore, there is no

need to consider the situation in Eq. (11). As a result, Eq. (1) is planar except that the two situations of Eq. (9) and Eq. (10).

Corollary 3. Let q be a power of odd prime p and consider the polynomial $f(x) \in \mathrm{F}_{q^3}[x]$ of the form

$$f(x) = x^{2q^2} + x^{2q} + x^2 + Ax^{q+1} + Bx^{q^2+1} + Cx^{q^2+q},$$

where $A, B, C \in \mathrm{F}_q$ and $A^2 + B^2 + C^2 - AB - AC - BC \neq 0$. Then, $f(x)$ is planar if and only if either of the followings holds

(i) $A + B + C \neq -2,$

(ii) $A + B + C \neq 6.$

Proof. We indicate that the cubic curve C defined by $F(X,Y) = 0$ is reducible when it satisfy either of the conditions (i) or (ii) in Lemma 1. By using

$$A^3 + B^3 + C^3 - 3ABC \neq -2(A^2 + B^2 + C^2 - AB - BC - AC)$$

from the condition (i) of Theorem 2 and the identity

$$A^3 + B^3 + C^3 - 3ABC = (A + B + C)(A^2 + B^2 + C^2 - AB - BC - AC).$$

Hence, we obtain

$$A + B + C \neq -2$$

since $A^2 + B^2 + C^2 - AB - AC - BC \neq 0.$ Similarly, using the following equation

$$A^3 + B^3 + C^3 - 3ABC \neq 6(A^2 + B^2 + C^2 - AB - BC - AC)$$

from the condition (ii) of Theorem 2 and the identity

$$A^3 + B^3 + C^3 - 3ABC = (A + B + C)(A^2 + B^2 + C^2 - AB - BC - AC),$$

we get

$$A + B + C \neq 6.$$

3. Conclusion and Future Work

Dembowski-Ostrom polynomials have important applications in many fields such as cryptography and coding theory. In this manuscript, we propose the complete classification of planar Dembowski-Ostrom polynomial of the form $f(x) = x^{2q^2} + x^{2q} + x^2 + Ax^{q+1} + Bx^{q^2+1} + Cx^{q^2+q}$ over F_{q^3} with odd characteristic, where $A, B, C \in \mathrm{F}_q$. For future research, we intend to use the method described in this manuscript or analogous algebraic function fields to obtain the planarity of certain Dembowski-Ostrom polynomials over field extensions greater than 3 or any field of characteristic 2.

Acknowledgment

This work was supported by Scientific Research Fund of Suleyman Demirel University. Project Number: FYL-2020-7985. The authors would like to express their gratitude to the anonymous reviewers for their invaluable suggestions.

Conflict of Interest

As the authors of this study, we declare that we do not have any conflict of interest statement.

Ethics Committee Approval and Informed Consent

As the authors of this study, we declare that we do not have any ethics committee approval and/or informed consent statement.

References

[1] D. Bartoli and M. Bonini, "Planar polynomials arising from linearized polynomials", *J. Algebra Appl.*, 21(1), 2250001, 2022.

[2] E. R. Berlekamp, *Algebraic coding theory (revised edition)*, World Scientific, 2015.

[3] A. Blokhuis, R. S. Coulter, M. Henderson and C. M. O'Keefe, "Permutations amongst the Dembowski-Ostrom polynomials," *Finite Fields and Applications*, Springer, Berlin, Heidelberg, , 2001. pp. 37-42.

[4] C. Carlet, C. Ding and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Trans. Inf. Theory*, 51, 2089-2102, 2005.

[5] R. S. Coulter and M. Henderson, "Commutative presemifields and semifields," *Adv. Math.*, 217, 282-304, 2008.

[6] R. S. Coulter and R. W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," *Des. Codes Cryptogr.*, 10, 167-184, 1997.

[7] P. Dembowski and T. G. Ostrom, "Planes of order n with collineation groups of order n^2," *Math. Z.*, 103, 239-258, 1968.

[8] U. Dempwolff, "More translation planes and semifields from Dembowski–Ostrom polynomials," *Des. Codes Cryptogr.*, 68, 81-103, 2013.

[9] C. Ding and H. Niederreiter, "Systematic authentication codes from highly nonlinear functions," *IEEE Trans. Inf. Theory*, 50, 2421-2428, 2004.

[10] C. Ding and J. Yin, "Signal sets from functions with optimum nonlinearity," *IEEE Trans. Comm.*, 55, 936-940, 2007.

[11] C. Ding and J. Yuan, "A family of optimal constant-composition codes," *IEEE Trans. Inf. Theory*, 51, 3668-3671, 2005.

[12] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problemy peredachi informatsii*, 21 3-16, 1985.

[13] G. Kyureghyan and F. Özbudak, "Planarity of products of two linearized polynomials", Finite Fields Their Appl., 18, 1076-1088, 2012.

[14] G. Kyureghyan, F. Özbudak, and A. Pott, "Some planar maps and related function fields," *Contemp.Math.*, 574, 87-114, 2012.

[15] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, 1997.

[16] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," *In Workshop on the Theory and Application of Cryptographic Techniques*, Berlin: Springer, 1989, pp. 549-562.

[17] K. Nyberg and L. R. Knudsen, "Provable security against a differential attack," *J. Cryptology*, 8, 27-37, 1995.

[18] K. Nyberg, "Perfect nonlinear S-boxes," *In Workshop on the Theory and Application of Cryptographic Techniques*, Springer, Berlin, Heidelberg, 1991, pp. 378-386.

[19] O. Ore, "Contributions to the theory of finite fields," *Trans. Am. Math. Soc.*, 36, 243-274, 1934.

[20] O. Ore, "On a special class of polynomials," *Trans. Am. Math. Soc.*, 35, 559-584, 1933.

[21] S. Puchinger and A. Wachter-Zeh, "Fast operations on linearized polynomials and their applications in coding theory," *J. Symbol. Comput.*, 89, 194-215, 2018.

[22] L. Ronyai and T. Szőnyi, "Planar functions over finite fields", *Combinatorica*, 9, 315-320, 1989.

[23] S. Samardjiska and D. Gligoroski, "Quadratic permutations, complete mappings and mutually orthogonal latin squares," *Math. Slovaca*, 67, 1129-1146, 2017.

[24] K. U. Schmidt and Y. Zhou, "Planar functions over fields of characteristic two," *J. Algebr. Combin.*, 40, 503-526, 2014.

[25] D. Silva, F. R. Kschischang and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory*, 54, 3951-3967, 2008.

[26] R. P. Singh, "Counterexamples to Dembowski and Ostrom conjecture on Planar function," arXiv preprint arXiv:2104.01942, 2021.

[27] X. Zhang, B. Wu and Z. Liu, "Dembowski-Ostrom polynomials from reversed Dickson polynomials," *J. Syst. Sci. Complex.*, 18, 259-271, 2016.

[28] Y. Zhou, "(2n,2n,2n,1)-Relative Difference Sets and Their Representations," *J. Comb. Des.*, 21, 563-584, 2013.