Journal of Research Administration
Society of Research Administrators International

NEW FAMILIES OF PLANAR FUNCTIONS OVER FINITE FIELDS OF EVEN CHARACTERISTIC

Dhananjay Kumar
Department of Mathematics, National Institute of Technology Patna, India.

Rajesh P. Singh*
Department of Mathematics, National Institute of Technology Patna, India.
Email: - rpsingh@cub.ac.in

Rishi Kumar Jha
Department of Mathematics, Central University of South Bihar, Gaya, India.

Abstract
A polynomial $f(x)$ over a finite field $\mathbb{F}_{2^n}$ is called a permutation polynomial if its associate function $f: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a bijective mapping. If $f(x+\theta)+f(x)+\theta x$ is a permutation polynomial of $\mathbb{F}_{2^n}$ for every non-zero $\theta \in \mathbb{F}_{2^n}$, then the polynomial $f(x)$ is said to be a planar function over $\mathbb{F}_{2^n}$. In this article, we propose two classes of planar functions over finite fields $\mathbb{F}_{2^{ts}}$ for $t = 3, 4$.

Keywords: Pseudo Planar functions, Planar functions, Linearized polynomials, Permutation polynomials.

1. Introduction

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements, where $q = p^n$ for some prime p and positive integer n. A polynomial f over a finite field $\mathbb{F}_q$ is called a permutation polynomial if its associated function $f: \mathbb{F}_q \to \mathbb{F}_q$ is one-one and onto. Permutation polynomials have attracted numerous researchers for more than a decade. Constructing new families of permutation polynomials and determining a given polynomial to be a permutation polynomial is a challenging problem [24]. Apart from this, permutation polynomials have been studied for their crucial applications in Cryptography [19, 20], Coding theory [3], Combinatorics [21] and many other disciplines.

In finite field theory, it is a well-known fact that any function $f: \mathbb{F}_q \to \mathbb{F}_q$ can be represented by a unique polynomial up to degree $q-1$ [12]. In this view, every function from a finite field $\mathbb{F}_q$ to itself is a polynomial over $\mathbb{F}_q$ and vice-versa. A polynomial f over finite field $\mathbb{F}_q$ is called planar if the polynomial $\mathfrak{D}_\theta(f(x)) = f(x+\theta) - f(x)$ is a permutation polynomial of $\mathbb{F}_q$ for every non-zero $\theta \in \mathbb{F}_q$. The polynomial $\mathfrak{D}_\theta(f(x))$ is called the discrete derivative of polynomial $f(x)$. The concept of planar function was first developed by P. Dembowski and T. G. Ostrom in 1968 [10]. They investigated projective planes with certain features using these functions. Numerous

attempts have been made to create new classes of planar function, but only a few classes have been identified so far. It is worth noting that all the known planar functions belong to a family $\phi(x) = \sum_{i,j=0}^{n-1} a_i\, x^{q^i+q^j}$ of polynomials called Dembowski- Ostrom (DO) Polynomial with only one exception $y^{\frac{3^s+1}{2}}$ in $\mathbb{F}_{3^k}$, where $s \geq 3$ is an odd number with $\gcd(s,k) = 1$ [8].

Let $\mathfrak{D}_\theta(f(x)) = f(x+\theta) - f(x) = \gamma$ has $n(\theta,\gamma)$ numbers of solutions for some $\gamma, \theta \in \mathbb{F}_q$. Consider $\Delta_f = max\{n(\gamma,\theta): \theta,\gamma \in \mathbb{F}_q, \theta \neq 0\}$. A function f is defined as differentially d-uniform if $\Delta_f = d$. In cryptography, functions with low differential uniformity are used due to their optimal resistance to differential cryptanalysis in block ciphers. In finite fields of even characteristics, the functions which are differential 2-uniform are called almost perfect nonlinear (APN) functions. The differential 1-uniform functions are called perfect nonlinear (PN) functions. It is easy to see that, PN functions are the planar functions itself and in Cryptographic terminology planar functions are referred as PN functions [5]. Such functions have also been used to construct linear codes. In 2005 [4], Carlet et.al. constructed error-correcting codes using perfect nonlinear functions and employed to construct secret sharing schemes. In 2016 [11], Chunlei and Helleseth derived several classes of p-array quasi-perfect codes using perfect nonlinear functions over finite fields. Apart from applications in cryptography and coding theory, planar polynomials have plenty of applications in combinatorics [1], design theory [18] and study of semifields [7]. Interested readers can see [15] for an excellent survey by Pott on planar and related functions.

It is easy to see that planar functions cannot exist over finite fields of even characteristic. Since, in this case, x and $x+\theta$ both satisfies $\mathfrak{D}_\theta(f(x)) = f(x+\theta) - f(x) = 0$. To handle this scarcity, functions with some similar properties have been investigated. For this purpose, Y. Zhou in 2013 [22] proposed a new definition of planar function over finite fields of even characteristic.

Definition 1.1. A function f: $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called a planar function or pseudo planar if $\mathfrak{D}_\theta\big(f(x)\big) = f(x+\theta) + f(x) + \theta x$ is a permutation of $\mathbb{F}_{2^n}$ for each non-zero $\theta \in \mathbb{F}_{2^n}$.

In last decade this topic has drawn attention of many researchers due to its many applications in mathematics and engineering. In 2014 [18], Schmidt and Zhou constructed a family of pseudo planar monomial ax^{2^k+1} over $\mathbb{F}_{q^2}$, where $q = 2^s$. Schere and Zieve constructed a monomial ax^{q^2+q} over finite field $\mathbb{F}_{2^{6s}}$ [17]. Beside the trivial pseudo planar monomial x^2, these two are the only example of pseudo planar monomials. Schmidt and Zhou conjectured that there are no more pseudo planar monomials. Several attempts have been made to construct and characterize the classes of pseudo planar functions. Hu et al. constructed two classes of pseudo planar binomials and used them to develop association schemes [10]. L. Qu developed an approach to determine pseudo planarity of some families of DO polynomials and constructed code books using pseudo planar function [16]. In 2021 [13], Li et al. characterized some families of binomials and trinomials over finite fields $\mathbb{F}_{2^{2m}}$, $\mathbb{F}_{2^{3m}}$, and $\mathbb{F}_{2^{4m}}$ for assuming m sufficiently large. Timpanella and Bartoli

characterized a family of binomials over $\mathbb{F}_{q^3}$ [2]. Abdukhalikov studied the pseudo planar functions in connection with mutually unbiased bases (MUBs) in combinatorics and proved that any pseudo planar function gives rise a semifield [1]. Constructing new families of pseudo planar functions is a challenging problem even though if they correspond to some existing semifields [16]. L. Qu constructed the optimal codebook which meets the Levenstein bound using the pseudo planar functions [16]. Apart from applications in coding theory, pseudo planar functions also have applications in finite geometry and combinatorics [22], [1].

Few classes of planar and pseudo planar functions are known so far. This strongly motivates the authors to construct new explicit families of pseudo planar functions over finite fields of even characteristic.

In section 2, we provide some preliminary results required for establishing the main results. In section 3, we propose two families of pseudo planar functions over $\mathbb{F}_{2^{tm}}$ for $t = 3, 4$.

2. Preliminary

The algebraic degree of a polynomial over a finite field of characteristic p is defined as maximum p weight of any exponent. For instance, the algebraic degree of Polynomial $g_1(x) = \sum_{i=0}^{n-1} a_i\, x^{q^i}$ over $\mathbb{F}_{q^n}$ is one, and the algebraic degree of the polynomial $g_2(x) = \sum_{i,j=0}^{n-1} a_i\, x^{q^i+q^j}$ over $\mathbb{F}_{q^n}$ is two.

Definition 2.2. Let $\mathbb{F}_{q^n}$ be the n −degree 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. So, the linearized polynomial $\mathfrak{L}(x)$ is 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.

Lemma 2.1. [8] The discrete derivative of a Dembowski-Ostrom polynomial is a linearized polynomial.

The next lemma provides a characterization of linearized polynomial to be a permutation polynomial.

Lemma 2.3. [12] Let $A = \begin{bmatrix} \alpha_0 & {\alpha_{n-1}}^q & \dots & {\alpha_1}^{q^{n-1}} \\ \alpha_1 & {\alpha_0}^q & \dots & {\alpha_2}^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1} & {\alpha_{n-2}}^q & \dots & {\alpha_0}^{q^{n-1}} \end{bmatrix}$

be a square matrix of order n, where $\alpha_i \in \mathbb{F}_{q^n}, i = 0,1 \cdots, n-1$. 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.

For $\alpha_i \in \mathbb{F}_q$ the matrix A reduces to the form $A = \begin{bmatrix} \alpha_0 & \alpha_{n-1} & \dots & \alpha_1 \\ \alpha_1 & \alpha_0 & \dots & \alpha_2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1} & \alpha_{n-2} & \dots & \alpha_0 \end{bmatrix}$.

The matrix A as defined above is called circulant matrix and it is usually denoted by $circ(\alpha_0, \alpha_1, \dots \alpha_{n-1})$.

Definition 2.4. [12] Let $\mathbb{F}_{q^n}$ be the extension field of $\mathbb{F}_q$. The trace of $\beta \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$, is a function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ defined as

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta) = \beta + \beta^q + \cdots + \beta^{q^{n-1}}.$$

If $\mathbb{F}_q$ is the prime subfield of $\mathbb{F}_{q^n}$ then trace is simply denoted by $Tr_{\mathbb{F}_{q^n}}(\beta)$ and called as absolute trace of β. The trace is a linear and balanced map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. It takes exactly q^{n-1} elements of $\mathbb{F}_{q^n}$ to a single element of $\mathbb{F}_q$ and in this way q^{n-1} elements of $\mathbb{F}_{q^n}$ has zero trace.

Lemma 2.5. [12] Let β be any element of $\mathbb{F}_{q^n}$. Then $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma) = 0$ if and only if γ is expressible as $\theta^q - \theta$ for some suitable $\theta \in \mathbb{F}_{q^n}$.

In the simplest case when $q = 2$, we see that for any $\gamma \in \mathbb{F}_{2^n}$, $Tr_{\mathbb{F}_{2^n}}(\gamma) = 0$ if and only if $\gamma = \theta^2 + \theta$ for some suitable $\theta \in \mathbb{F}_{2^n}$.

3. Families of Pseudo Planar functions

In this section we present our classes of pseudo planar functions. Throughout the Section, we take $q = 2^m$.

In this section we present our classes of pseudo planar functions. Throughout the Section, we take $q = 2^m$.

Theorem 3.1. Let u, v, and δ are elements of $\mathbb{F}_q$ with $\delta = u^6 + v^6$**.** Then the polynomial $f(x) = \frac{uv^5}{\delta} x^{q+1} + \frac{u^5 v}{\delta} x^{q^2+1} + \frac{u^3 v^3}{\delta} x^{q^2+q}$ is a pseudo planar over $\mathbb{F}_{q^3}$ if $u^3 + v^3 \neq 0$.

Proof. For any $\theta \in \mathbb{F}^*_{q^3}$ consider the polynomial $\mathfrak{D}_\theta(f(x)) = f(x+\theta) + f(x) + f(\theta) + \theta x$. The polynomial $f(x)$ is a pseudo planar if and only if $\mathfrak{D}_\theta(f(x))$ is a permutation polynomial of $\mathbb{F}_{q^3}$. We have,

$$\mathfrak{D}_\theta(f(x)) = \frac{uv^5}{\delta}(x\theta^q + x^q\theta) + \frac{u^5v}{\delta}\left(x\theta^{q^2} + x^{q^2}\theta\right) + \frac{u^3v^3}{\delta}\left(x^{q^2}\theta^q + x^q\theta^{q^2}\right)$$

$$= \{uv^5\theta^q + u^5v\theta^{q^2} + \delta\theta\}x + \{uv^5\theta u^3v^3\theta^{q^2}\}x^q + \{u^5v\theta + u^3v^3\theta^q\}x^{q^2}$$

$$= \{uv^5\theta^q + u^5v\theta^{q^2} + (u^6+v^6)\theta\}x + \{uv^5\theta + u^2v^4\theta^q + u^2v^4\theta^q + u^3v^3\theta^{q^2}\}x^q$$

$$+\{u^5v\theta + u^4v^2\theta^{q^2} + u^4v^2\theta^{q^2} + u^3v^3\theta^q\}x^{q^2}$$

$$= \{u^5\left(v\theta^{q^2} + u\theta\right) + v^5(u\theta^q + v\theta)\}x + \{uv^4(v\theta + u\theta^q) + u^2v^3\left(v\theta^q u\theta^{q^2}\right)\}x^q$$

$$+\{u^4v\left(u\theta + v\theta^{q^2}\right) + u^3v^2\left(u\theta^{q^2} + v\theta^q\right)\}x^{q^2}.$$

The polynomial $\mathfrak{D}_\theta(f(x))$ is a linearized polynomial. Let α be any solution of $\mathfrak{D}_\theta(f(x)) = 0$. In view of Lemma 2.3, it suffices to show that $\alpha = 0$. On the contrary, suppose $\alpha \neq 0$.

$$Tr\left(\mathfrak{D}_\theta(f(\alpha))\right) = Tr\left(u^5\left(u\theta + v\theta^{q^2}\right)\alpha + uv^4(v\theta + u\theta^q)\alpha^q + u^3v^2\left(u\theta^{q^2} + v\theta^q\right)\alpha^{q^2}\right)$$

$$+Tr\left(v^5(u\theta^q + v\theta)\alpha + u^2v^3\left(u\theta^{q^2} + v\theta^q\right)\alpha^q + u^4v\left(u\theta + v\theta^{q^2}\right)\alpha^{q^2}\right)$$

$$= (u^5 + uv^4 + u^3v^2)Tr\left(\left(u\theta + v\theta^{q^2}\right)\alpha\right) + (v^5 + u^2v^3 + u^4v)Tr\left(\left(u\theta + v\theta^{q^2}\right)\alpha^{q^2}\right)$$

$$= \frac{u^6+v^6}{(u+v)^2}Tr\left(\left(u\theta + v\theta^{q^2}\right)\left(\alpha u + v\alpha^{q^2}\right)\right)$$

Since, $\mathfrak{D}_\theta(f(\alpha)) = 0$, this implies that $Tr\left(\mathfrak{D}_\theta(f(\alpha))\right) = 0$. In view of *Lemma 2.3*, it follows that $u\theta + v\theta^{q^2}$ is a permutation polynomial for every non-zero $\theta \in \mathbb{F}_{q^3}$, thus $u\theta + v\theta^{q^2}$ represents an arbitrary non zero element of $\mathbb{F}_{q^3}$. This implies that every non zero element of $\mathbb{F}_{q^3}$ has trace zero. This is a contradiction. Therefore, we have $\alpha = 0$. This completes the proof.

Theorem 3.2. Let $u, v,$ and δ are elements of $\mathbb{F}_q$ with $\delta = u^8 + v^8$, and $u \neq v$. Then, the polynomial $f(x) = \frac{uv^7}{\delta}x^{q+1} + \frac{u^7v}{\delta}x^{q^3+1} + \frac{u^3v^5}{\delta}x^{q^2+q} + \frac{u^5v^3}{\delta}x^{q^3+q^2}$ is a pseudo planar function over $\mathbb{F}_{q^4}$.

Proof. Let θ be an arbitrary non-zero element of $\mathbb{F}_{q^4}$. $f(x)$ is a planar polynomial if $\mathfrak{D}_\theta(f(x)) = f(x+\theta) + f(x) + f(\theta) + \theta x$ is a permutation polynomial.

$$\mathfrak{D}_\theta(f(x)) = \frac{uv^7}{\delta}(x^q\theta + x\theta^q) + \frac{u^7v}{\delta}\left(x^{q^3}\theta + x\theta^{q^3}\right) + \frac{u^3v^5}{\delta}\left(x^{q^2}\theta^q + x^q\theta^{q^2}\right)$$

$$+\frac{u^5v^3}{\delta}\left(x^{q^3}\theta^{q^2} + x^{q^2}\theta^{q^3}\right)$$

Ignoring the factor $\frac{1}{\delta}$ and rearranging the terms, we have,

$$\mathfrak{D}_\theta(f(x)) = \left(uv^7\theta^q + \delta\theta + u^7v\theta^{q^3}\right)x + \left(uv^7\theta + u^3v^5\theta^{q^2}\right)x^q + \left(u^3v^5\theta^q + u^5v^3\theta^{q^3}\right)x^{q^2}$$

$$+\left(u^7v\theta + u^5v^3\theta^{q^2}\right)x^{q^3}$$

$$= \left(uv^7\theta^q + u^8\theta + v^8\theta + u^7v\theta^{q^3}\right)x + \left(uv^7\theta + u^2v^6\theta^q + u^2v^6\theta^q + u^3v^5\theta^{q^2}\right)x^q$$

$$+\left(u^3v^5\theta^q + u^4v^4\theta^{q^2} + u^4v^4\theta^{q^2} + u^5v^3\theta^{q^3}\right)x^{q^2}$$

$$+\left(u^7v\theta + u^6v^2\theta^{q^3} + u^6v^2\theta^{q^3} + u^5v^3\theta^{q^2}\right)x^{q^3}$$

$$= \{u^7\left(u\theta + v\theta^{q^3}\right) + v^7(v\theta + u\theta^q)\}x + \{uv^6(v\theta + u\theta^q) + u^2v^5\left(v\theta^q + u\theta^{q^2}\right)\}x^q$$

$$+\{u^3v^4\left(v\theta^q + u\theta^{q^2}\right) + u^4v^3\left(v\theta^{q^2} + u\theta^{q^3}\right)\}x^{q^2}$$

$$+\{u^6v\left(v\theta^{q^2} + u\theta\right) + u^5v^2\left(v\theta^{q^2} + u\theta^{q^3}\right)\}x^{q^3}$$

$$= \{u^7\left(u\theta + v\theta^{q^3}\right)x + uv^6(u\theta^q + v\theta)x^q + u^3v^4\left(u\theta^{q^2} + v\theta^q\right)x^{q^2}$$

$$+u^5v^2\left(u\theta^{q^3} + v\theta^{q^2}\right)x^{q^2}\} + \{v^7(v\theta + u\theta^q)x + u^2v^5\left(v\theta^q + u\theta^{q^2}\right)x^q$$

$$+u^4v^3\left(v\theta^{q^2} + u\theta^{q^3}\right)x^{q^2} + u^6v\left(v\theta^{q^3} + u\theta\right)x^{q^2}\}$$

Next,

$$Tr\left(\mathfrak{D}_\theta(f(x))\right) = Tr\{u^7\left(u\theta + v\theta^{q^3}\right)x + uv^6(u\theta^q + v\theta)x^q + u^3v^4\left(u\theta^{q^2} + v\theta^q\right)x^{q^2}$$

$$+u^5v^2\left(u\theta^{q^3} + v\theta^{q^2}\right)x^{q^2}\} \qquad +Tr\{v^7(v\theta + u\theta^q)x + u^2v^5\left(v\theta^q + u\theta^{q^2}\right)x^q$$

$$+u^4v^3\left(v\theta^{q^2} + u\theta^{q^3}\right)x^{q^2} + u^6v\left(v\theta^{q^3} + u\theta\right)x^{q^2}\}$$

$$= (u^7 + uv^6 + u^3v^4 + u^5v^2)Tr\left(\left(u\theta + v\theta^{q^3}\right)x\right)$$

$$+\left(v^7 + u^{[2]}v^5 + u^4v^3 + u^6v\right)Tr\left(\left(u\theta + v\theta^{q^3}\right)x^{q^3}\right)$$

$$= (u^6 + v^6 + u^2v^4 + u^4v^2)\{Tr\left(\left(u\theta + v\theta^{q^3}\right)ux\right) + Tr\left(\left(u\theta + v\theta^{q^3}\right)vx^{q^3}\right)\}$$

$$= (u + v)^6 Tr\left(\left(u\theta + v\theta^{q^3}\right)\left(ux + vx^{q^3}\right)\right).$$

Next, following the arguments of Theorem 3.1 completes the proof.

References

1. K. Abdukhalikov, "Symplectic spreads, planar functions, and mutually unbiased bases," J. Algebraic Comb., vol. 41 pp.1055-1077 ,2015.
2. D. Bartoli and M. Timpanella, A family of planar binomials in characteristic 2, Finite Fields Appl., vol. 63, pp. 101651, 2020.
3. Y. L. Chapuy, Permutation polynomials and applications to coding theory Finite Fields Appl. Vol. 13, pp. 58–70, 2007.
4. C. Carlet, C. Ding, J. Yuan, Linear codes from perfect nonlinear mappings and their secret sharing schemes, IEEE Trans. Inf. Theory, vol. 51, no. 6, pp. 2089-2102, 2015.
5. C′., Blondean, K. Nyberg, Perfect nonlinear functions and Cryptography, Finite Fields Appl., vol. 32, pp. 120-147, 2015.
6. R. S. Coulter, On the classification of planar monomials over fields of square order Finite Fields Appl., vol. 18 pp. 316-336, 2012.
7. R. S. Coulter, M. Henderson, Commutative presemifields and semifields Advances in Mathematics, vol. 217, pp. 282-304, 2008.
8. R. S. Coulter, R. W. Matthews, Planar functions and planes of Lenz–Barlotti class II, Des. Codes Cryptogr., vol. 10, pp. 168-184, 1997.
9. P. Dembowski, T. G. Ostrom. Planes of order n with collineation groups of order n^2, Math. eit., vol. 103, pp. 239-258, 1968.
10. S. Hu, S. Li, T. Zhang, T. Feng and G. Ge, New Pseudo-Planar Binomials in Characteristic Two and Related Schemes, Des.Codes Cryptoger., vol. 76, pp. 345-360 2015.
11. C. Li, T. Helleseth, Quasi-perfect linear codes from planar and APN functions, Cryptogr. Commun., vol. 8, no. 2, pp. 215-227, 2016.
12. R. Lidl, H. Niederreiter Finite Fields, Encyclopaedia of mathematics and its Applications Cambridge University Press
13. Y. Li, K. Li, L. Qu and C. Li, Further study of planar functions in field of characteristic two, journal of Algebra, vol. 573, pp. 712-740, 2021.
14. G. L. Mullen, D. Panario, Handbook of Finite Fields, CRC Press, Taylor & Francis Group, 2013.
15. A. Pott, Almost perfect and planar functions, Des. Codes Crypto., vol. 78, pp. 141-195, 2016.
16. L. Qu, A new approach to constructing quadratic pseudo planar function over $\mathbb{F}_2 n$.,
17. IEEE rans. Inf. Theory, vol. 62, no. 11, pp. 6644-6658, 2016.
18. Z. Scherr and M. E. Zieve, Some planar monomials in characteristic 2, Ann.Comb., vol. 18, pp. 723-729, 2014.

19. K.-U. Schmidt, Y. Zhou. Planar functions over fields of characteristic two, J Alg. Comb. Vol. 40, pp. 503–526, 2014.
20. R. P. Singh, A. Saikia, B. K. Sarma. Poly-dragon: an efficient multivariate public key cryptosystem Journal of Mathematical Cryptology, vol. 4, no. 4, 2011. [20] R. P. Singh, B. K. Sarma, A. Saikia. A Public Key Cryptosystem using a group of permutation polynomials, Tatra Mt. Math. Publ., vol. 77, pp. 139-162, 2020. [21] R. P. Singh, M. K. Singh Two congruence identities on ordered partitions,
21. INTEGERS: A journal of Combinatorial Number Theory, A73, vol. 18, 2018.
22. Y. Zhou, (2n, 2n, 2n, 1)-relative difference sets and their representations. J. Combin. Des. Vol. 21, pp. 563–584, 2013.
23. Z. Zhou and X. Tang, “New Nearly Optimal Codebooks from Relative Difference Sets,” Adv. in Math. Communications, vol. 5, no. 3, 521-527, 2011.
24. Xiang-dong Hou, Permutation polynomials over finite fields-A survey of recent advances, Finite Fields Appl., vol. 32, pp. 82-119, 2015.