symmetry

MDPI

Article

Construction of Permutation Polynomials Using Additive and Multiplicative Characters

Varsha Jarali [1], Prasanna Poojary [2] and Vadiraja G. R. Bhatta [1,*]

[1] Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576014, India; varshapjarali@gmail.com or varsha.jarali@learner.manipal.edu
[2] Department of Mathematics, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal 576014, India; poojaryprasanna34@gmail.com or poojary.prasanna@manipal.edu
* Correspondence: vadiraja.bhatta@manipal.com

Abstract: Permutation is a natural phenomenon useful for understanding and explaining the structural and functional behavior of objects or concepts. The mathematical formulation of permutation behavior can be readily achieved by permutation polynomials. Permutation polynomials are constructed by suitably modifying linearized polynomials and associated affine polynomials with the help of additive characters, multiplicative characters, and special types of Trace functions for the polynomials in one and more than one indeterminates. The permutation properties of the obtained polynomials are verified using the AGW criterion.

Keywords: permutation polynomial; trace function; AGW criteria; planar functions

check for updates

Citation: Jarali, V.; Poojary, P.; Bhatta, V.G.R. Construction of Permutation Polynomials Using Additive and Multiplicative Characters. *Symmetry* **2022**, *14*, 1539. https://doi.org/10.3390/sym14081539

Academic Editor: Mihai Postolache

Received: 4 June 2022
Accepted: 11 July 2022
Published: 27 July 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Some usual and natural processes such as ordering and re-ordering, arrangements, and derangements make a remarkable difference in many real-life situations. Various scientific developments require a sensible study of combinatorial designs involving permutations and combinations, which lead to a special branch of mathematics. Over the last 50 years, the theory of finite fields has been a widely discussed branch of algebra due to its diverse application in coding theory, cryptography, and various number-theoretic and combinatorial aspects. Starting from the 17th century, the subject has taken its own part in mathematical concepts, including theoretical, computational, scientific, and technical interests. Eminent mathematicians like Fermat, Euler, Lagrange, and Legendre contributed to the structure theory of finite prime fields. Carl Friedrich Gauss and Evariste Galois worked independently in making the classical general theory of finite fields, which exposed remarkably to the emergence of discrete mathematics and modern number theory as serious algebraic serious disciplines.

Investigation and various applications of finite fields require the theoretic study of polynomials over finite fields as an important tool. It is possible to express any non-constant polynomial over a finite field as a product of all irreducible polynomials. It is required to devise some algorithms which are reasonably efficient for the actual computation of irreducible factors of any polynomial of the positive degree over a finite fields. Beyond the concern of finite fields, the factorization of polynomials is also useful in many algebraic and number-theoretic computational problems in one or the other way.

It is possible to represent any function mapped from a finite field to itself by a polynomial over a finite field. Thus, finite fields are polynomially complete. It is obviously natural to expect the permutation of a finite set of elements in combinatorial study or any such studies in discrete mathematics. The advantage of finite fields over other finite sets is due to the scope of the algebraic study of permutation of elements, which can be achieved through polynomial permutations. Hermite started the initial study of permutation polynomials over finite prime fields and the concept has been continuously explored

by many researchers in recent years, including the construction of permutation polynomials and application of permutation polynomials to finite projective geometry or various such mathematical concepts as well as cryptographic applications of permutation polynomials. The most important step was taken by Zieves [1] and his lemma became a powerful tool to construct many old and new kinds of permutation polynomials.

2. Preliminary

A polynomial $f(x) \in F_q[x]$ is called a permutation polynomial over the finite field F_q if the associated polynomial with it is a mapping $f : c \to f(c)$ from F_q to F_q is a bijection. A polynomial p in n variables, $x_1, x_2, \ldots x_n$ is symmetric if for any permutation $\sigma \in S_n$, $p(x_1, x_2, \ldots x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$. In [2] Wan proved that if $f(x)$ is exceptional over $\mathbb{F}_q$, then $f(x)$ is a permutation polynomial over $\mathbb{F}_q$ by way of p-adic lifting lemma and Newton's formula about symmetric polynomials. Let $f \in \mathbb{F}_q[x]$ be a polynomial of degree n such that $1 \leq n \leq q$ and let s_k be the kth elementary symmetric polynomial of values $f(c)$, that is,

$$\prod_{c \in \mathbb{F}_q} (x - f(c)) = \sum_{k=0}^{q} (-1)^k s_k x^{q-k}.$$

By studying elementary symmetric polynomials, Turnwald [3] proved a theorem giving nine characterizations of permutation polynomials. He also gave a very simple and elementary proof of Wan's theorem ([2], Theorem 2.1) based on an elementary symmetric polynomial. Ensuring that a given polynomial is a permutation polynomial, there are several criteria with rather complicated conditions to satisfy. In [4], the additive character is used to prove $F(x) = G(x) + \gamma Tr(H(x))$ is permutation polynomial over F_{2^n}. In [5] complete permutation polynomials are constructed in four classes using additive character. In [6] evaluated class of the Weil sum using additive character. By applying some known results as in [7] and AGW Criterion [8], we have obtained several new types of permutation polynomials using the existence of almost one solution of $f(x) = d$ for any $d \in F_{q^n}$.

In [9–13], Yaun and Zeng investigated permutation polynomials in the form $(x^{2^m} + x + \delta)^s + x$ with different cases of m and s. Similarly in [10,14,15], Yaun and Zha developed polynomials $(x^{p^m} - x + \delta)^s + x$ which are over the field F_{2^n}. Jose et al. in [16] considered permutation polynomials with Carlitz rank 2 and developed a sharp lower bound for the weight of any PP polynomials. In [17] Vadiraja et al. investigated permutation polynomials over finite rings with respect to the sequences they generate. The sequences generated by various permutation polynomials are tested for randomness using well-known statistical methods. In [18] Sartaj et al. discussed c-differential uniformity and boomerang uniformity using additive characters of two classes of permutation polynomials. We have been inspired by [6] the method they have used and additive characters and its property to find Weil sum.

For $n \geq 1$, let $F_q[x_1, x_2, \ldots, x_n]$ be a ring of polynomial in n-indeterminates over F_q. In [19], they constructed permutation polynomial of n-indeterminates using additive and multiplicative characters over a finite ring. In [20], they discussed the relationship between planar functions and a permutation polynomial in n-indeterminates. Permutation polynomials have many applications in cryptography [21–25] coding theory [26–28] and combinatorial designs [29]. Permutations polynomials can be used as public-key cryptosystem, Rajesh et al. [30] proposed little dragon two cryptosystems by using permutation polynomials as a public key cryptosystem. In [23], Rajesh et al. proposed an efficient multivariate encryption scheme with the help of a group of permutation polynomials over finite fields, proposed cryptosystem was secure against usual known attacks on existing multivariate public-key cryptosystems. Khachatrian et al. [25] developed a new public-key encryption system based on permutation polynomials using permutation polynomials as a public polynomial for encryption.

In this paper, we have considered additive characters, multiplicative characters, Jacobi sum, and AGW Criterion to construct a new kind of permutation polynomials in one

and more than one indeterminates and also proved affine polynomial is not a planar function. Quadratic forms have a major role to play in theory and methods of optimization. The criterion, recently discovered by Akbary et al. [8] (AGW) is a simple and effective method that establishes the permutation property of a mapping $F_{q^n} \to F_{q^n}$ through a commutative diagram. The main proofs in this paper completely depend on AGW Criterion and existence of at most one solution for the equation $f(x) = d$ for each $d \in F_q$, where $x \in F_q$. To have completeness in this section we discuss some of the results related to them. As a prerequisite to understanding and developing the theory, we need the existing definitions and results, which are listed here. In the following section, we made use of these concepts as tools for our work.

Lemma 1 ([31]). *The necessary and sufficient condition for a polynomial $f(x) \in F_q[x]$ to be a permutation of F_q is any one of the following four conditions;*

1. *$f : c \to f(c)$ is surjective*
2. *$f : c \to f(c)$ is injective*
3. *The equation $f(x) = a$ has a solution in F_q for each $a \in F_q$*
4. *For each $a \in F_q$, the equation $f(x) = a$ has a unique solution in F_q.*

Lemma 2 (**The AGW Criterion:** [8]). *If the maps g, $\bar{g}$, ω and $\bar{\omega}$ such that $g : K \to K$, $\bar{g} : L \to \bar{L}$, $\omega : K \to L$, and $\bar{\omega} : K \to \bar{L}$ with $\bar{\omega} \circ g = \bar{g} \circ \omega$ and both ω and $\bar{\omega}$ surjective, where K, L and $\bar{L}$ be finite sets with $|L| = |\bar{L}|$ [Figure 1]. Then, the following statements are equivalent:*

1. *g is a bijection from K to K.*
2. *$\bar{g}$ is a bijection from L to $\bar{L}$ and g is injective on $\omega^{-1}(l)$ for each $l \in L$.*

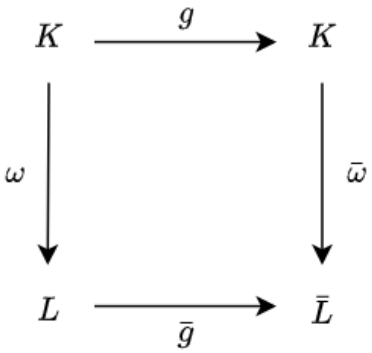


Figure 1. Given statement is symbolized using the diagram.

The major proofs in this work are based on the AGW Criterion, which simplifies the challenge of proving permutation polynomials over F_{q^n} to that of proving permutation polynomials over its subfield F_q.

Trace functions are widely used in different types of concepts over finite fields. For properties of trace one can refer [31].

Definition 1 ([31]). *The trace $Tr_{q^n/q}(\alpha)$ over F_q for any $\alpha \in F_{q^n}$ is defined as $Tr_{q^n/q}(\alpha) = \sum_{i=0}^{m} \alpha^{q^i}$.*

We use the following definition defined in [32].

Definition 2 ([32]). *Let $f(x) = \sum_{i=0}^{m} a_i x^i \in F_{q^n}[x]$ with coefficients $a_i \in F_{q^n}$ then $T[f](x) = Tr(f(x)) = \sum_{i=0}^{m} Tr(a_i)x^i$.*

Definition 3 ([31]). *The character function $\chi_1(c) = e^{\frac{2\pi i Tr(c)}{p}}$ defined on additive group of F_q is known as canonical additive character of F_q.*

Definition 4 ([31]). *The function χ_b with $\chi_b(c) = \chi_1(bc)$ for all $b, c \in F_{q^n}$ is known as additive character of F_{q^n}.*

By setting, $b = 0$ in above definition we get trivial additive character χ_0, such that $\chi_0(c) = 1$ for all $c \in F_{q^n}$.

Definition 5 ([31]). *A polynomial $L(x)$ with the coefficients in an extension field F_{q^n} of the field F_q represented as*

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

is known as $q-$ linearized polynomial over F_{q^n}.

Definition 6 ([31]). *A polynomial in the form $A(x) = L(x) - \alpha$ where $L(x)$ is a linearized polynomial over F_{q^n} and $\alpha \in F_{q^n}$, is an affine polynomial over F_{q^n}.*

Definition 7 ([33]). *If for every $b \in F_q^*$, the function $f(x+b) - f(x)$ is a permutation of F_q, then $f : F_q \to F_q$ is known as a planar function.*

The number of solutions of a polynomial function and properties of additive characters are interrelated to observe the permutation behavior of polynomials. We state the following results from [31], which we readily used in our work.

Theorem 1 ([31]). *A mapping $g : F_{q^n} \to F_{q^n}$ is a permutation polynomial if and only if for every $\alpha \in F_{q^n}^*$*

$$\sum_{x \in F_{q^n}} (-1)^{Tr(\alpha g(x))} = 0.$$

Theorem 2 ([31]). *If χ is a non-trivial additive character of the finite field F_{q^n} then $\sum_{g \in F_{q^n}} \chi(g) = 0$.*

Remark 1 ([31]). *For any $d \in F_{q^n}$*

$$N = \frac{1}{q} \sum_{c \in F_{q^n}} \sum_{\chi} \chi(f(c)) \bar{\chi}(d). \tag{1}$$

is the number of solutions of $f(x) = d$ in F_{q^n}.

Some of the required definitions and theorems to construct permutation polynomial in n-indeterminates are listed below.

Definition 8 ([31]). *A polynomial $f(x_1, \ldots, x_n)$ over F_q is known as a permutation polynomial in n indeterminates, if for each $a \in F_q$, the equation $f(x_1, \ldots, x_n) = a$ has q^{n-1} solutions in F_q^n .*

Definition 9 ([31]). *Let $g \in F_q$ be a fixed primitive element. The function ψ_j for each $j = 0, 1, \ldots, q-2$, is a multiplicative character of F_q with*

$$\psi_j(g^k) = e^{2\pi ijk/(q-1)} \quad for \quad k = 0, 1, \ldots, q-2.$$

ψ_0 is a trivial multiplicative character if $\psi_0(c) = 1$ for all $c \in F_q^*$.

Definition 10 ([31]). *When q is odd, the quadratic character of F_q is a real valued function η on F_q^* with*

$$\eta(c) = \begin{cases} 0 & \text{if } c = 0 \\ 1 & \text{if } c \text{ is square of an element of } F_q^* \\ -1 & \text{otherwise.} \end{cases}$$

Definition 11 ([31]). *The function v on F_q is integer valued function if $v(b) = -1$ for $b \in F_q^*$ and $v(0) = q - 1$.*

Lemma 3 ([31]). *For any finite field F_q we have*

$$\sum_{c \in F_q} v(c) = 0 \tag{2}$$

and for any $b \in F_q$,

$$\sum_{c_1 + c_2 + \ldots + c_n = b} v(c_1)v(c_2)\cdots v(c_k) = \begin{cases} 0 & if 1 \le k \le m \\ v(b)q^{m-1} & if k = m \end{cases} \tag{3}$$

where the sum is over all $c_1, c_2, \ldots, c_m \in F_q$ with $c_1 + c_2 + \ldots c_m = b$.

Definition 12 ([31]). *Let $\gamma_1, \ldots, \gamma_k$ be k multiplicative characters of F_q. Then the sum*

$$J(\gamma_1, \ldots, \gamma_k) = \sum_{c_1 + c_2 + \ldots + c_n = 1} \gamma_1(c_1)\cdots\gamma_k(c_k), \tag{4}$$

with the summation extended over all $k-$ tuples $(c_1, \ldots, c_k)$ of elements of F_q satisfying $c_1 + c_2 + \ldots + c_n = 1$, is called a Jacobi sum in F_q.

Definition 13 ([31]). *The homogeneous polynomial of degree 2, or the zero polynomial $f(x_1, \ldots, x_n) \in F_q[x_1, \ldots, x_n]$ is a quadratic form in n indeterminates over F_q if,*

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j \;\; with \;\; a_{ij} = a_{ji} \;\; for \;\; 1 \le i \le j \le n.$$

Theorem 3 ([31]). *Every quadratic form over F_q, q odd, is equivalent to a diagonal quadratic form.*

3. Construction of Permutation Polynomials Using Additive Character

In this section we construct the polynomials of the type $f(x) = a_t x^{q^t} + a_{t-1}x^{q^{t-1}} + \ldots + a_1 x^q + a_0 x + a$ and $P(x) = f(Tr(x)) + k(Tr(x)) \cdot T[h](x)$. We prove these two type of polynomials are permutation polynomials based on the additive character over F_{q^n}.

Theorem 4. *The affine polynomial $f(x) = a_t x^{q^t} + a_{t-1}x^{q^{t-1}} + \ldots + a_1 x^q + a_0 x + a$ is a permutation polynomial over the finite field F_{q^n} of characteristic p.*

Proof. It is enough to prove that $f(x) = d$ has atmost one solution in F_{q^n}. We make use of additive character over F_{q^n} and $\sum_{c \in F_{q^n}} \chi_b(f(c)) = \sum_{c \in F_{q^n}} \chi_b(L(c) + a) = \sum_{c \in F_{q^n}} [\chi_b(a) + \chi_1(L(c))] = \chi_b(a)\sum_{c \in F_{q^n}} \chi_1(L(c))$ where $L(x) = ba_t x^{q^t} + ba_{t-1}x^{q^{t-1}} + \ldots + ba_1 x^q + ba_0 x$ is a $q-$ polynomial over F_{q^n}.

Put $\tau(c) = \chi_1(L(c)$ for all $c \in F_{q^n}$, by the property of $L(c)$ implies that $\tau(c)$ is an additive character of F_{q^n}. Thus,

$$\sum_{c\in F_{q^n}} \chi_1(L(c)) = \sum_{c\in F_{q^n}} \tau(c) = \begin{cases} q & \text{if } \tau \text{ is trivial} \\ 0 & \text{if } \tau \text{ is nontrivial.} \end{cases}$$

From the above Remark 1,

$$\begin{aligned} N = \frac{1}{q}\sum_{c\in F_{q^n}}\sum_{\chi_b}\chi_b(f(c))\overline{\chi_b(d)} &= \frac{1}{q}\sum_{c\in F_{q^n}}\sum_{\chi_b}\chi_b(d)\chi_1(L(c))\overline{\chi_b(d)} \\ &= \frac{1}{q}\sum_{c\in F_{q^n}}\chi_1(L(c)) = \frac{1}{q}\sum_{c\in F_{q^n}}\tau(c) \end{aligned}$$

Hence $f(x) = d$ has atmost one solution in F_{q^n}. □

Example 1. *$a_2x^2 + a_1x + a_0$ is a permutation polynomial over F_{q^n} with q even.*

Proposition 1. *Let F_{2^n} be a finite field of characteristic 2 and $f(x) = a_tx^{2^t} + a_{t-1}x^{2^{t-1}} + \ldots + a_1x^2 + a_0x + a$ be an affine polynomial over F_{2^n}. For $g(x) \in F_{2^n}[x]$ and $a \in F_{2^n}$, the polynomial $F(x) = f(x) + aTr(g(x))$ is a permutation polynomial over F_{2^n} if and only if for all $\lambda \in F_{2^n}^*$,*

$$\sum_{x\in F_{2^n}} (-1)^{Tr(\lambda a)[1+Tr(g(x))]} = 0 \quad \textit{whenever} \quad \sum_{i=0}^{t} a_i = 0,$$

$$\textit{and} \sum_{x\in F_{2^n}} (-1)^{Tr(\lambda a)[1+Tr(g(x))]+\lambda Tr(x)} = 0 \quad \textit{whenever} \quad \sum_{i=0}^{t} a_i = 1.$$

Proof. If $L(x)$ is a linearised polynomial then $f(x) = L(x) + a$ is an affine polynomial over F_{2^n} for any $a \in F_{2^n}$ and $tr(f(x)) = Tr(a) + (a_0 + a_1 + \ldots + a_t)Tr(x)$. Hence, $Tr(\lambda F(x)) = Tr(\lambda a)[1 + Tr(g(x))] + \lambda(a_0 + a_1 + \ldots + a_t)Tr(x)$.

By Theorem 1 $F(x)$ is a permutation polynomial if and only if $\sum_{x\in F_{2^n}}(-1)^{Tr(\lambda F(x))} = 0$ for all $\lambda \in F_{2^n}^*$.

Combining these facts together we can write,

$$\sum_{x\in F_{2^n}} (-1)^{Tr\lambda F(x)} = \begin{cases} \sum_{x\in F_{2^n}}(-1)^{Tr(\lambda a)[1+Tr(g(x))]} = 0 & \text{if } \sum_{i=0}^{n} a_i = 0 \\ \sum_{x\in F_{2^n}}(-1)^{Tr(\lambda a)[1+Tr(g(x))]+\lambda Tr(x)} = 0 & \text{if } \sum_{i=0}^{n} a_i = 1 \end{cases}$$

which completes the proof. □

Thus the affine polynomial $f(x) = a_tx^{q^t} + a_{t-1}x^{q^{t-1}} + \ldots + a_1x^q + a_0x + a$ over F_{q^n} is a good candidate to be a permutation polynomial. But using the Definition 7, we observe that the same function is not a planar function, which is shown in the following result.

Theorem 5. *An affine polynomial $f(x) = a_tx^{q^t} + a_{t-1}x^{q^{t-1}} + \ldots + a_1x^q + a_0x + a$ over F_{q^n} is not planar function over F_{q^n}.*

Proof. The function $f(x)$ is planar if $f(x + b) - f(x)$ permutes F_{q^n} for all $b \in F_{q^n}^*$. Here we need to show that $f(x + b) - f(x)$ does not permute F_{q^n}

In fact, $f(x + b) - f(x)$

$$\begin{aligned} &= a_r(x+b)^{q^t} + a_{r-1}(x+b)^{q^{t-1}} + \ldots + a_1(x+b)^q + a_0(x+b) + a - \\ &(a_tx^{q^t} + a_{t-1}x^{q^{t-1}} + \ldots + a_1x^q + a_0x + a) \end{aligned}$$

As F_{q^n} is a field of characteristic p, this expression reduces to

$$a_r b^{q^t} + a_{r-1} b^{q^{t-1}} + \ldots + a_0 b = L(b),$$

which is a constant, which shows that $f(x+b) - f(x)$ cannot be a permutation of the field. □

Reis and Wang [32] defined $T[f](x)$ as shown in Definition 2 with the help of a polynomial $f(x) \in F_{q^n}[x]$ using Trace function. Here we construct another type of permutation polynomial with the help of $T[f](x)$.

Theorem 6. *Let $P(x) = f(Tr(x)) + k(Tr(x)) \cdot T[h](x)$ where $f(x), k(x) \in F_{q^n}[x]$, and $T[h](x) \in F_q[x]$ with $h(x) \in F_q[x]$ and $k(Tr(F_{q^n})) \subseteq F_q^*$. Then $P(x)$ is a permutation polynomial if $Tr(\lambda) = 0$ for all $\lambda \in F_q^*$.*

Proof. By AGW Criterion $P(x)$ is a permutation polynomial over F_{q^n} if and only if $Q(x) = T[f](x) + k(x) \cdot T[h](x)$ is a permutation polynomial over F_q. The given statement is symbolized using the diagram Figure 2.

From the Theorem 1 for each $\lambda \in F_q^*$,

$$\sum_{x \in F_q} (-1)^{Tr(\lambda Q(x))} = \sum_{x \in F_q} (-1)^{Tr(\lambda) T[f](x) + Tr(\lambda) k(x) \cdot T[h](x)}$$

$$= \sum_{x \in F_q} (-1)^{Tr(\lambda)\{T[f](x) + k(x) T[h](x)\}}$$

This sum is zero if $Tr(\lambda) = 0$, which completes the proof. □

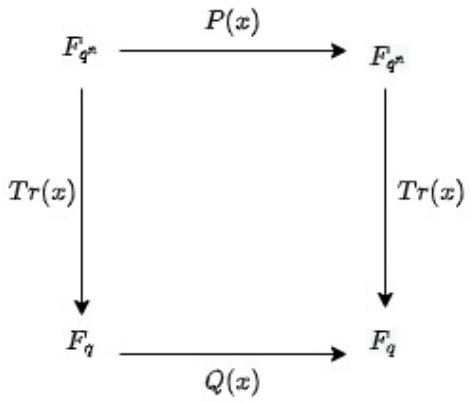


Figure 2. Theorem is symbolized using the diagram.

Corollary 1. *Let $P(x) \in F_{q^n}[x]$ and m be an odd positive integer such that $P(x) = f(Tr(x)) + T[h](x)$, where $f(x) \in F_{q^n}[x]$ is of degree m and $T[h](x) \in F_q[x]$ with $h(x) \in F_q[x]$. If $Tr(f(Tr(y))) = 0$, for all $y \in F_{q^n}$ then $P(x)$ is a permutation polynomial over F_{q^n}.*

Proof. By taking $k(x) = 1$ in the previous theorem, $Q(x)$ reduces to $Q(x) = T[f](z) + T[h](z) = T[h](z)$, for each $z \in Tr(F_{q^n})$. By AGW Criterion $P(x)$ is permutation polynomial if and only if $Q(x)$ is permutation polynomial. Here $Q(x)$ being a $p-$ polynomial will be bijective when m is odd. □

4. Permutation Polynomials in *n*-Indeterminates

In this section, we construct permutation polynomials in n-indeterminates using multiplicative character, Jacobi sum, and quadratic form-related properties.

Theorem 7. *Let F_q be a finite field of characteristic p. Let $f(x_1, \ldots, x_n)$ be a quadratic form over F_q, with n indeterminates and odd q. Then $f(x_1, \ldots, x_n)$ is a permutation polynomial over F_q^n if at least one of the coefficients a_i of the corresponding diagonal quadratic form is zero.*

Proof. Being a quadratic form $f(x_1, \ldots, x_n)$ is always equivalent to the diagonal quadratic form $a_1x_1^2 + \ldots + a_nx_n^2$. Thus it is enough to show that $a_1x_1^2 + \ldots + a_nx_n^2 = b$ has exactly q^{n-1} solutions for each $b \in F_q$.

Using trivial multiplicative character ψ_0 and quadratic character η, with $c_1, c_2, \ldots, c_n \in F_q^n$, the number of solutions of $a_1x_1^2 + \ldots + a_nx_n^2$ can be computed as

$$\begin{aligned}
&N(a_1x_1^2 + \ldots + a_nx_n^2)\\
&= \sum_{c_1+c_2+\ldots+c_n=b} N(a_1x_1^2 = c_1)N(a_2x_2^2 = c_2)\cdots N(a_nx_n^2 = c_n)\\
&= \sum_{c_1+c_2+\ldots+c_n=b} [1+\eta(c_1a_1^{-1})][1+\eta(c_2a_2^{-1})]\cdots[1+\eta(c_na_n^{-1})]\\
&= \sum_{c_1+c_2+\ldots+c_n=b} [\psi_0(c_1a_1+\eta(c_1a_1))][\psi_0(c_2a_2)+\eta(c_2a_2)]\cdots[\psi_0(c_na_n)+\eta(c_na_n)]\\
&= \psi_0(a_1)\cdots\psi_0(a_n)J_b(\psi_0,\ldots,\psi_0) + \eta(a_1,\ldots,(a_n))J_b(\eta,\ldots,\eta)\\
&= q^{n-1} + \eta(a_1\cdots a_n)J_b(\eta,\ldots,\eta)
\end{aligned} \tag{5}$$

If n is even and $b \neq 0$,

$$J(\eta,\ldots,\eta) = -q^{(\frac{n-2}{2})}\eta[(-1)^{\frac{n}{2}}]$$

so that

$$N = q^{n-1} - q^{(\frac{n-2}{2})}\eta[(-1)^{\frac{n}{2}}a_1\cdots a_n]$$

If n is odd and $b \neq 0$,

$$J(\eta,\ldots,\eta) = -q^{(\frac{n-1}{2})}\eta[(-1)^{\frac{n-1}{2}}]$$

so that

$$N = q^{n-1} - q^{(\frac{n-1}{2})}\eta[(-1)^{\frac{n-1}{2}}ba_1\cdots a_n].$$

In both of the above cases if $\prod_{i=1}^{n} a_i$ is zero, the number of solutions will be q^{n-1} for each $b \in F_q^*$.

When $b = 0$,

$$J(\eta,\ldots,\eta) = -q^{(\frac{n-2}{2})}\eta[(-1)^{\frac{n}{2}}]$$

and hence the number of solutions will be q^{n-1} . □

Corollary 2. *For odd q, the quadratic form f over F_q is permutation polynomial over F_q^2 if $a_1a_2 = 0$.*

Proof. Let $f(x_1, x_2)$ be a quadratic form over F_q. It is equivalent to $a_1x_1^2 + a_2x_2^2 = b$ for $b \in F_q$.

With $c_1, c_2 \in F_q$ we obtain,

$$\begin{aligned}
N(a_1x_1^2 + a_2x_2^2 = b) &= \sum_{c_1+c_2=b} N(a_1x_1^2 = c_1)N(a_2x_2^2 = c_2)\\
&= \sum_{c_1+c_2=b} [1+\eta(c_1a_1^{-1})][1+\eta(c_2a_2^{-1})] = q + \eta(a_1a_2)J_b(\eta,\eta).
\end{aligned}$$

If $a_1a_2 = 0$ then $\eta(a_1a_2) = 0$ and hence, $N = q$ □

Theorem 8. *Let F_q be a finite field with q even. For odd n*

$$x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} + ax_n^2$$

is a permutation polynomial over F_q^n.

Proof. It is enough to show that

$$N(x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} + ax_n^2 = b)$$

has q^{n-1} solutions over F_q^n for each $b \in F_q$.

$$\begin{aligned} &N(x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} + ax_n^2 = b) \\ &= \sum_{c_1+c_2=b} N(x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} = c_1)N(ax_n^2 = c_2) \end{aligned} \tag{6}$$

$N(x_1x_2 = b)$ is $q-1$ if $b \neq 0$ and $2q-1$ if $b = 0$. These two cases can be combined as $N(x_1x_2 = b) = q + v(b)$. So we have, $N(x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} = c_1) = q^{n-2} + v(c_1)q^{\frac{n-3}{2}}$. And by using the property of diagonal quadratic form,

$N(ax_n^2 = c_2) = N(x_n^2 = a^{-1}c_2) = \lambda(a^{-1}c_2) = \lambda(a^{-1})J_b(\lambda) = q^{1-1} = 1$. Hence from the Equation (6),

$$N = \sum_{c_1+c_2=b} (q^{n-2} + v(c_1)q^{\frac{n-3}{2}}) \cdot 1 = q^{n-1} + q^{\frac{n-3}{2}} \sum_{c_1+c_2=b} v(c_2) = q^{n-1}. \tag{7}$$

□

Theorem 9. *For odd n and even q, the quadratic form*

$$x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} + x_n^2$$

is a permutation polynomial over F_q^n.

Proof. It is enough to show that

$$N(x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} + x_n^2 = b)$$

has q^{n-1} solutions over F_q^n for each $b \in F_q$.

Let f be a quadratic form equivalent to

$$f(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij}x_ix_j$$

Suitable non-singular linear substitution for indeterminates will be the same in the cases of either some a_{ii} being zero or all a_{ii} being zero.

Without loss of generality assuming $a_{12} \neq 0$, the non singular linear substitution will be

$$\begin{aligned} x_2 &= a_{12}^{-1}(y_2 + a_{13}y_3 + \ldots + a_{1n}y_n) \\ x_i &= y_i \ \ for \ \ i \neq 2 \end{aligned}$$

Hence by assigning arbitrary values to $x_1, x_2, \ldots, x_{n-1}$ and the corresponding value of x_n,

$$N(x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} + x_n^2 = b) = q^{n-1}.$$

□

The following result is to prove that $f(x_1, x_2, \ldots, x_n) = x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} + x_n^2$ is not a planar function using nontrivial additive character of F_q.

Theorem 10. *Let F_q be a finite field with q even. For odd n*

$$x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} + x_n^2$$

is not a planar function over F_q^n.

Proof. Let $f(x_1, x_2, \ldots, x_n) = x_1x_2 + x_3x_4 + \ldots + x_{n-2}x_{n-1} + x_n^2$.
Then for $(a_1, a_2, \ldots, a_n) \in F_q^n$,

$$f(x_1 + a_1, x_2 + a_2, \ldots, x_n + a_n) - f(x_1, x_2, \ldots, x_n) = a_1a_2 + a_3a_4 + \ldots + a_n^2,$$

which is a constant. This shows that $f(x_1, x_2, \ldots, x_n)$ cannot be a planar function. □

5. Conclusions

Permutation of finite field elements is a useful property that increases the richness of finite fields. The construction of such polynomials has become a major part of research in recent years. We contributed a notable work of construction of Permutation polynomials using additive characters, multiplicative characters, and Trace functions for the polynomials in one and more than one indeterminates. The AGW criterion is effectively used to understand the permutation behavior of the constructed polynomials. Linearised polynomials and associated affine polynomials can be suitably modified to form permutation polynomials. The construction of planar functions may also be an interesting work using a similar method in the future.

Author Contributions: Conceptualization, V.G.R.B. and V.J.; methodology, V.G.R.B.; validation, V.G.R.B., V.J., and P.P.; formal analysis, V.J.; writing original draft preparation, V.J.; writing review and editing, V.G.R.B. and P.P.; visualization, P.P.; supervision, V.G.R.B. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by Manipal Academy of Higher Education, Manipal, India.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the editor and referees for their valuable comments and suggestions, which improved the quality of this article. The corresponding author acknowledges the Manipal Institute of Technology (MIT), Manipal Academy of Higher Education, India, for their kind encouragement. The first author is grateful to UGC-CSIR Grant Commission for their support through Grant N0.201610069412 and the Manipal Academy of Higher Education for their kind encouragement and support. The second author acknowledges the Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, India, for their kind encouragement.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zieve, M. On some permutation polynomials over of the form $x^r h(x^{\frac{q-1}{d}})$. *Proc. Am. Math. Soc.* **2009**, *137*, 2209–2216. [CrossRef]
2. Wan, D. A p-adic lifting lemma and its application to permutation polynomials. *Recall* **1993**, *1*, 1.
3. Turnwald, G. A new criterion for permutation polynomials. *Finite Fields Their Appl.* **1995**, *1*, 64–82. [CrossRef]
4. Charpin, P.; Kyureghyan, G.M. On a Class of Permutation Polynomials over F_{q^2}. In Proceedings of the International Conference on Sequences and Their Applications, Lexington, KY, USA, 14–18 September 2008; pp. 368–376.
5. Wu, G.; Li, N.; Helleseth, T.; Zhang, Y. Some classes of monomial complete permutation polynomials over finite fields of characteristic two. *Finite Fields Their Appl.* **2014**, *28*, 148–165. [CrossRef]
6. Coulter, R.S. On the evaluation of a class of Weil sums in characteristic 2. *N. Zeal. J. Math* **1999**, *28*, 171–184.

7. Kyureghyan, G.; Zieve, M. Permutation polynomials of the form X+ γTr (Xk). In *Contemporary Developments in Finite Fields and Applications*; World Scientific: Singapore, 2016; pp. 178–194.
8. Akbary, A.; Ghioca, D.; Wang, Q. On constructing permutations of finite fields. *Finite Fields Their Appl.* **2011**, *17*, 51–67. [CrossRef]
9. Yuan, J.; Ding, C. Four classes of permutation polynomials of F_{2^m}. *Finite Fields Their Appl.* **2007**, *13*, 869–876. [CrossRef]
10. Yuan, J.; Ding, C.; Wang, H.; Pieprzyk, J. Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$. *Finite Fields Their Appl.* **2008**, *14*, 482–493. [CrossRef]
11. Zeng, X.; Zhu, X.; Hu, L. Two new permutation polynomials with the form $(x^p - x + \delta)^s + L(x)$. *Appl. Algebra Eng. Commun. Comput.* **2010**, *21*, 145–150. [CrossRef]
12. Yuan, P.; Ding, C. Permutation polynomials over finite fields from a powerful lemma. *Finite Fields Their Appl.* **2011**, *17*, 560–574. [CrossRef]
13. Tu, Z.; Zeng, X.; Jiang, Y. Two classes of permutation polynomials having the form $(x^{2^m} + x + \delta)^s + x$. *Finite Fields Their Appl.* **2015**, *31*, 12–24. [CrossRef]
14. Yuan, P.; Ding, C. Further results on permutation polynomials over finite fields. *Finite Fields Their Appl.* **2014**, *27*, 88–103. [CrossRef]
15. Zha, Z.; Hu, L. Some classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x$ over $F_{p^{2m}}$. *Finite Fields Their Appl.* **2016**, *40*, 150–162. [CrossRef]
16. Oliveira, J.A.; Martínez, F.B. Permutation polynomials with Carlitz rank 2. *Discret. Math.* **2021**, *344*, 112155. [CrossRef]
17. Vadiraja Bhatta, G.; Shankar, B.; Mishra, V.N.; Poojary, P. Sequences of numbers via permutation polynomials over some finite rings. *Proyecciones* **2020**, *39*, 1295–1313. [CrossRef]
18. Hasan, S.U.; Pal, M.; Stănică, P. The c-differential uniformity and boomerang uniformity of two classes of permutation polynomials. *IEEE Trans. Inf. Theory* **2021**, *68*, 679–691. [CrossRef]
19. Shaofang, H. Additive characters and orthogonal systems of polynomials in several indeterminates over residue class rings. *Chin. Sci. Bull.* **1998**, *43*, 275–277. [CrossRef]
20. Nakagawa, N. On polynomial families in n indeterminates over finite prime fields coming from planar functions. In *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 251–262.
21. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
22. Singh, R.P.; Sarma, B.; Saikia, A. Public key cryptography using permutation p-polynomials over finite fields. *Cryptol. Eprint Arch.* **2009**, *2009*, 208.
23. Singh, R.P.; Sarma, B.K.; Saikia, A. A public key cryptosystem using a group of permutation polynomials. *Tatra Mt. Math. Publ.* **2020**, *77*, 139–162. [CrossRef]
24. Singh, R.P.; Saikia, A.; Sarma, B. Poly-dragon: An efficient multivariate public key cryptosystem. *J. Math. Cryptol.* **2011**, *4*, 349–364. [CrossRef]
25. Khachatrian, G.; Kyureghyan, M. Permutation polynomials and a new public-key encryption. *Discret. Appl. Math.* **2017**, *216*, 622–626. [CrossRef]
26. Ding, C.; Zhou, Z. Binary cyclic codes from explicit polynomials over GF (2m). *Discret. Math.* **2014**, *321*, 76–89. [CrossRef]
27. Ding, C. Cyclic codes from some monomials and trinomials. *SIAM J. Discret. Math.* **2013**, *27*, 1977–1994. [CrossRef]
28. Laigle-Chapuy, Y. Permutation polynomials and applications to coding theory. *Finite Fields Their Appl.* **2007**, *13*, 58–70. [CrossRef]
29. Ding, C.; Yuan, J. A family of skew Hadamard difference sets. *J. Comb. Theory Ser. A* **2006**, *113*, 1526–1535. [CrossRef]
30. Singh, R.P.; Saikia, A.; Sarma, B. Little dragon two: An efficient multivariate public key cryptosystem. *arXiv* **2010**, arXiv:1005.5028.
31. Lidl, R.; Niederreiter, H. *Finite Fields*; Number 20; Cambridge University Press: Cambridge, UK, 1997.
32. Reis, L.; Wang, Q. Permutation polynomials from a linearized decomposition. *arXiv* **2021**, arXiv:2104.13234.
33. Dembowski, P.; Ostrom, T.G. Planes of ordern with collineation groups of ordern 2. *Math. Z.* **1968**, *103*, 239–258. [CrossRef]