ON PERMUTATION POLYNOMIALS OVER FINITE FIELDS

by

ESEN AKSOY

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabanci University
Fall 2006

ON PERMUTATION POLYNOMIALS OVER FINITE FIELDS

APPROVED BY

Prof. Dr. Alev Topuzoğlu .....
(Thesis Supervisor)

Prof. Dr. Plamen Borrisov Djakov .....

Assist. Prof. Dr. Cem Güneri .....

Assist. Prof. Dr. Albert Levi .....

Assoc. Prof. Dr. Wilfried Meidl .....

DATE OF APPROVAL: .....

to my parents and brother

Acknowledgements

First of all, I would like to express my deepest gratitude to my supervisor Prof. Dr. Alev Topuzoğlu for her friendliness since the first day we met. Her understanding and great vision has helped me to find my way throughout my studies at Sabanci University.

I also thank Assoc. Prof. Dr. Wilfried Meidl who have asssisted me during the work of this thesis.

I am also grateful to my friends in the Mathematics Program and to Alp, Serkan, Meltem, Erhan, Emel, Malima, and Erol for their invaluable friendship and encouragement.

Finally, many thanks goes to my family for their love, and endless support.

ON PERMUTATION POLYNOMIALS OVER FINITE FIELDS

Esen Aksoy

Mathematics, Master of Science Thesis, 2006

Thesis Supervisor: Prof. Dr. Alev Topuzoğlu

Keywords: permutation polynomials, finite fields, binomials, monomials, Dickson polynomials, symmetric group of degree n.

Abstract

A permutation polynomial (PP) over a finite field $\mathbb{F}_q$ is a polynomial in $\mathbb{F}_q[x]$ which induces a bijective map from $\mathbb{F}_q$ to itself. PPs are of great theoretical interest and are also needed for applications.

This thesis starts with some basic facts about PPs. Recent results about one of the most important open problems in this topic: counting PPs of a given degree, are presented.

Well known classes of PPs are the linear polynomials, the monomials x^k, with $gcd(k, q-1) = 1$, the linearized polynomials, and the Dickson polynomials. It turns out that finding new classes of PPs is not easy. We also focus on this problem and give a survey of some recent constructions.

SONLU CİSİMLER ÜZERİNDE PERMÜTASYON POLİNOMLARI

Esen Aksoy

Matematik, Yüksek Lisans Tezi, 2006

Tez Danışmanı: Prof. Dr. Alev Topuzoğlu

Anahtar Kelimeler: permütasyon polinomu, sonlu cisim, Dickson polinomları, derecesi n olan simetrik grup.

Özet

Sonlu bir cisim $\mathbb{F}_q$ üzerindeki bir permütasyon polinomu (PP), $\mathbb{F}_q$ dan $\mathbb{F}_q$ ya birebir ve örten bir fonksiyondur. PP ları teorik açıdan büyük önem taşımakta ve aynı zamanda uygulamalarda da kullanılmaktadır.

Bu tez PP ları hakkında temel bazı bilgilerle başlamaktadır. Bu konuyla ilgili açık problemlerden biri olan "verilen bir derecedeki PP larının sayısı" üzerinde son zamanlarda yapılmış olan çalışmalar incelenmektedir.

Doğrusal polinomlar, $(k, q-1) = 1$ koşulunu sağlayan x^k formundaki polinomlar ve Dickson polinomları bilinen bazı PP sınıflarıdır. Yeni PP sınıflarını bulmanın kolay bir problem olmadığı bilinmektedir. Bu tezde son zamanlarda bu problem üzerinde elde edilen sonuçlara da yer verilmiştir.

Contents

CHAPTER 1

INTRODUCTION

Permutation polynomials (PP) over finite fields play important role in the study of secure transmission of data and in combinatorics for the construction of several combinatorial designs. Throughout this thesis, we intend to give a survey of some recent theoretical results on PPs over finite fields. For a detailed literature on this subject we refer to the books [8] and [12], and to the article [10].

In this Chapter, we first introduce the well known criterion for the determination of PPs and review some of the known classes of PPs.

1.1 Preliminaries

Definition 1.1.1. Let $\mathbb{F}_q$ be a finite field of q elements, where $q = p^n$, p is a prime and n is a positive integer. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be a PP of $\mathbb{F}_q$ if the induced map $\alpha \to f(\alpha)$ from $\mathbb{F}_q$ to itself is bijective.

Given a permutation σ of the elements of $\mathbb{F}_q$, there exists a unique polynomial $f_\sigma \in \mathbb{F}_q[x]$ with $deg(f_\sigma) < q$ and $f_\sigma(c) = \sigma(c)$ for all $c \in \mathbb{F}_q$. The polynomial f_σ can be given by the formula

$$f_\sigma(x) = \sum_{c \in \mathbb{F}_q} \sigma(c)(1 - (x - c)^{q-1}). \tag{1.1}$$

or by the Lagrange interpolation formula, see for instance [8]. From (1.1), we note that $deg(f_\sigma) \leq q - 2$, since all elements of $\mathbb{F}_q$ sum up to zero.

Consider an (arbitrary) polynomial $f \in \mathbb{F}_q[x]$. One can asscociate f to the reduction polynomial $g \in \mathbb{F}_q[x]$ by taking $f \mod (x^q - x)$, since g and f induce the same map over $\mathbb{F}_q$, as stated in the following lemma.

Lemma 1.1.1. *For $f, g \in \mathbb{F}_q[x]$, $f(c) = g(c)$ for all $c \in \mathbb{F}_q$ if and only if $f(x) \equiv g(x) \mod (x^q - x)$.*

Proof. Using divison algorithm we have, $f(x) - g(x) = h(x)(x^q - x) + r(x)$ for some $h, r \in \mathbb{F}_q[x]$ with $deg(r) < q$. Substituting c for x, we get $f(c) = g(c)$ for all $c \in \mathbb{F}_q$ if and only if $r(c) = 0$ for all $c \in \mathbb{F}_q$, which is equivalent to $r = 0$. □

1.2 Analysis of Permutation Polynomials

In order to classify PPs over finite fields, one needs some criteria to test whether a given polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation of $\mathbb{F}_q$ or not. Among these criteria, in some sense, the most useful one was given by Hermite for prime fields, which was then generalized by Dickson to finite fields $\mathbb{F}_q$, where q is a prime power.

Theorem 1.2.1. *(Hermite's Criterion)*
Let $\mathbb{F}_q$ be a finite field of characteristic p. A polynomial $f(x) \in \mathbb{F}_q[x]$ is a PP of $\mathbb{F}_q$ if and only if the following two conditions are satisfied:

(i) *f has exactly one root in $\mathbb{F}_q$,*

(ii) *For each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \mod p$, the reduction of $f(x)^t \mod (x^q - x)$ has degree $\leq q-2$.*

See [8] for the proof.

Corollary 1.2.1. *If $d > 1$ is a divisor of $q-1$, then there is no PP of $\mathbb{F}_q$ of degree d.*

Proof. Let $f \in \mathbb{F}_q[x]$ with $deg(f) = d$. Then there exists $1 \leq t = (q-1)/d \leq q-2$ such that $f(x)^t \mod (x^q - x)$ has degree $q-1$. Therefore by Hermite's Criterion, we conclude that f is not a permutation polynomial of $\mathbb{F}_q$. □

Using additive characters, we state another criterion.

Theorem 1.2.2. *The polynomial $f \in \mathbb{F}_q[x]$ is a PP of $\mathbb{F}_q$ if and only if*

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = 0,$$

for all nontrivial additive characters χ of $\mathbb{F}_q$

Proof. We first recall that an additive character χ of $\mathbb{F}_q$ is defined by

$$\chi = \chi(x) = e^{2\pi i Tr(ax)/p},\ a \in \mathbb{F}_q.$$

where $Tr(\alpha)$ denotes the (absolute) trace $Tr : \mathbb{F}_q \to \mathbb{F}_p$, defined by

$$Tr(\alpha) = \alpha + \alpha^p + ... + \alpha^{p^{n-1}}.$$

From the properties of characters of a finite abelian group, it follows that if χ is any nontrivial additive character of $\mathbb{F}_q$, then

$$\sum_{c \in \mathbb{F}_q} \chi(c) = 0.$$

Now let f be a PP of $\mathbb{F}_q$ and χ be a nontrivial character of $\mathbb{F}_q$. Then

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = \sum_{c \in \mathbb{F}_q} \chi(c) = 0.$$

For the converse, assume that $\sum_{c \in \mathbb{F}_q} \chi(f(c)) = 0$ for all nontrivial additive characters χ of $\mathbb{F}_q$. We can give the number of solutions $f(x) = a$ in $\mathbb{F}_q$ for any $a \in \mathbb{F}_q$ by

$$\frac{1}{q} \sum_{c \in \mathbb{F}_q} \sum_{\chi} \chi(f(c))\overline{\chi(a)} = 1 + \frac{1}{q} \sum_{\chi \neq \chi_0} \overline{\chi(a)} \sum_{c \in \mathbb{F}_q} \chi(f(c)) = 1,$$

where we used the so-called *orthogonality of characters*:

$$\sum_{c \in \mathbb{F}_q} \chi_c(a)\overline{\chi_c(b)} = \begin{cases} q & \text{if } a = b \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, f is a PP of $\mathbb{F}_q$. □

1.3 Main Classes of Permutation Polynomials

(1) Every linear polynomial $ax + b \in \mathbb{F}_q[x]$, $a \neq 0$, is a PP of $\mathbb{F}_q$.

Proof. Every linear polynomial over $\mathbb{F}_q$ is one to one, the rest follows from the definition of PPs. □

(2) The monomial x^k is a PP of $\mathbb{F}_q$ if and only if $gcd(k, q-1) = 1$.

Proof. If a is an element of $\mathbb{F}_q$ of order m, then $| < a^k > | = \frac{m}{gcd(k,m)}$. Therefore, the function $c \to c^k$ from $\mathbb{F}_q$ to $\mathbb{F}_q$ is onto if and only if $gcd(k, q-1) = 1$. □

(3) Let $\mathbb{F}_q$ be an extension field of $\mathbb{F}_p$ of degree n. Then, the *linearized polynomial*

$$L(x) = \sum_{i=0}^{n} a_i x^{p^i} \in \mathbb{F}_q[x]$$

is a PP of $\mathbb{F}_q$ if and only if 0 is the only root of $L(x) \in \mathbb{F}_q$.

Proof. Since we have $L(ax + y) = aL(x) + L(y)$ for all $x, y \in \mathbb{F}_q$, and $a \in \mathbb{F}_p$, L is a linear operator on $\mathbb{F}_q$. Hence, for L to be one-to-one, it is necessary and sufficient that 0 is the only root of $L(x)$ in $\mathbb{F}_q$. □

(4) *Dickson Polynomials (of the 1st kind)* defined by the formula

$$D_k(x,a) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}, \tag{1.2}$$

where $a \in \mathbb{F}_q$, also constitute a class of PPs.

The Dickson polynomial of the 1st kind $D_k(x,a) \in \mathbb{F}_q[x]$, $a \in \mathbb{F}_q^*$, is a PP of $\mathbb{F}_q$ if and only if $gcd(k, q^2-1) = 1$.

Proof. Let $gcd(k, q^2-1) = 1$ and $D_k(b,a) = D_k(c,a)$ for some $b, c \in \mathbb{F}_q$. Let α, β be the roots of $x^2 - bx + a$ and $x^2 - cx + a$, respectively, in $\mathbb{F}_{q^2}$. Then α, β satisfy the equations $\alpha + a\alpha^{-1} = b$, $\beta + a\beta^{-1} = c$, so that

$$D_k(\alpha + a\alpha^{-1}, a) = D_k(\beta + a\beta^{-1}, a).$$

Then, from the "functional equation" (see for example [8])

$$D_k(x + \frac{a}{x}, a) = x^k + \frac{a^k}{x^k} \tag{1.3}$$

it follows that

$$\alpha^k + a^k\alpha^{-k} = \beta^k + a^k\beta^{-k},$$

$$(\alpha^k\beta^k - a^k)(\alpha^k - \beta^k) = 0.$$

Hence, either $\alpha^k = \beta^k$ or $\alpha^k = (a\beta^{-1})^k$. Since $gcd(k, q^2-1) = 1$, x^k is a permutation polynomial of $\mathbb{F}_{q^2}$. So we have $\alpha = \beta$ or $\alpha = a\beta^{-1}$, and both cases give us b=c. Therefore, $D_k(x,a)$ is a PP of $\mathbb{F}_q$.

For the converse, assume that $D_k(x,a)$ is a PP of $\mathbb{F}_q$ and $gcd(k, q^2-1) = d$ where $d > 1$. If d is even, then k is even and q is odd. But then, from (1.2) it follows that all powers of x in $D_k(x,a)$ are even. So, we get $D_k(b,a) = D_k(-b,a)$ for all $b \in \mathbb{F}_q^*$, which is a contradiction to our assumption, since q is odd and therefore $char(\mathbb{F}_q) \neq 2$. Therefore d is odd and there exists an odd prime divisor r of d such that $r|\ k$ and $r|\ q^2-1$. We consider the following two cases:

Case 1 Let $r|\ k$ and $r|\ q-1$. Since all roots of $x^r - 1$ are the elements of $\mathbb{F}_q$, there exists an element $\alpha \neq 1, a \in \mathbb{F}_q$ with $\alpha^r = 1$. Then $\alpha^k = 1$ and

$$D_k(\alpha + a\alpha^{-1}, a) = \alpha^k + \frac{a^k}{\alpha^k} = 1 + a^k = D_k(1+a, a).$$

Knowing that $D_k(x,a)$ is a PP of $\mathbb{F}_q$, we have $\alpha + a\alpha^{-1} = 1 + a$ implying $\alpha = 1$ or $\alpha = a$ which is impossible by the choice of α.

Case 2 Let $r|\ k$ and $r|\ q+1$. Let α be a root of $x^{q+1}-a$ in $\mathbb{F}_{q^2}$. Since x^r-1 has r roots in $\mathbb{F}_{q^2}$, we can choose a root β of x^r-1 with $\beta \neq 1, a\alpha^{-2}$. Using $\beta^k = 1$, we can write,

$$\alpha^k + \frac{a^k}{\alpha^k} = \beta^k\alpha^k + \frac{a^k}{\beta^k\alpha^k},$$
$$D_k(\alpha + a\alpha^{-1}, a) = D_k(\beta\alpha + a(\beta\alpha)^{-1}, a),$$

where the second identity follows from (1.3). But since α is a root of $x^{q+1}-a$, it follows that

$$\alpha + a\alpha^{-1} \quad = \quad \alpha + \alpha^q.$$

On the other hand,

$$\begin{aligned}(\alpha+\alpha^q)^q &= \alpha^q + \alpha^{q^2} \\ &= \alpha^q + \alpha\end{aligned}$$

which shows that $\alpha + \alpha^q \in \mathbb{F}_q$. Therefore,

$$\alpha + a\alpha^{-1} = \alpha + \alpha^q \in \mathbb{F}_q.$$

Similarly

$$\beta\alpha + a(\beta\alpha)^{-1} = \beta\alpha + (\beta\alpha)^q \in \mathbb{F}_q.$$

Now considering the assumption that $D_k(x,a)$ is a PP of $\mathbb{F}_q$, we would have

$$\alpha + a\alpha^{-1} = \beta\alpha + a(\beta\alpha)^{-1}$$

implying $\beta = 1$ or $\beta = a\alpha^{-2}$ which is impossible by the choice of β.

Hence, we conclude that $gcd(k, q^2-1) = 1$. □

Remark 1.3.1. Since $D_k(x,0) = x^k$, the Dickson polynomials can be considered as the generalization of the power polynomials. We also note that $deg(D_k(x,a)) = k$ and for a given Dickson polynomial $D_k(x,a)$ over $\mathbb{F}_q$, being a permutation of $\mathbb{F}_q$ is only dependent on k.

A monic polynomial f is said to be in *normalized form* if f is of the form:

$$f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x \in \mathbb{F}_q[x]$$

and when the characteristic p does not divide n, then $a_{n-1} = 0$.

Given a PP $f(x)$ of $\mathbb{F}_q$, we can reduce it to the normalized form by composing it with a suitable linear polynomial $g(x) = ax + b \in \mathbb{F}_q[x]$. Hence, rather than general

class of PPs it is convenient to just study PPs in normalized form. In Table below, which can be found in [11], we give the Dickson's lists of all normalized PPs of degree at most 6, on account of Hermite's Criterion. We note that generalization of these polynomials to higher degrees is still an unsolved problem.

Normalized PP of $\mathbb{F}_q$	q
x	any q
x^2	$q \equiv 0 \bmod 2$
x^3	$q \not\equiv 1 \bmod 3$
$x^3 - ax$(a not a square)	$q \equiv 0 \bmod 3$
$x^4 \pm 3x$	$q = 7$
$x^4 + a_1x^2 + a_2x$(if its only root in $\mathbb{F}_q$ is 0)	$q \equiv 0 \bmod 2$
x^5	$q \not\equiv 1 \bmod 5$
$x^5 - ax$(a not a fourth power)	$q \equiv 0 \bmod 5$
$x^5 + ax(a^2 = 2)$	$q = 9$
$x^5 \pm 2x^2$	$q = 7$
$x^5 + ax^3 \pm x^2 + 3ax^2$($a$ not a square)	$q = 7$
$x^5 + ax^3 + 5^{-1}a^2x$(a arbitrary)	$q \equiv \pm 2 \bmod 5$
$x^5 + ax^3 + 3a^2x$(a not a square)	$q = 13$
$x^5 - 2ax^3 + a^2x$(a not a square)	$q \equiv 0 \bmod 5$
$x^6 \pm 2x$	$q = 11$
$x^6 \pm a^4x^3 + a^2x^2 \pm 5x(a \neq 0)$	$q = 11$
$x^6 \pm 4a^2x^3 + ax^2 \pm 4x$($a = 0$ or a not a square)	$q = 11$

Lemma 1.3.1. *Let $f(x), g(x) \in \mathbb{F}_q[x]$. Then the composition $f(g(x))$ is a bijection of $\mathbb{F}_q$ if and only if $f(x)$ and $g(x)$ are bijections of $\mathbb{F}_q$.*

Proof. Let $f(x)$ and $g(x)$ be bijections of $\mathbb{F}_q$. Then if $f(g(x_1)) = f(g(x_2))$, then $g(x_1) = g(x_2)$ implying $x_1 = x_2$. Conversely assume that $f(g(x))$ is a bijection of $\mathbb{F}_q$. If $f(x)$ is not a bijection, that is not onto, then $f(g(x))$ can not be onto, contradicting to $f(g(x))$ being a bijection of $\mathbb{F}_q$. Now let $g(x_1) = g(x_2)$. Then, $f(g(x_1)) = f(g(x_2))$, implying that $x_1 = x_2$. Therefore $f(x)$ and $g(x)$ are bijections of $\mathbb{F}_q$. □

Lemma 1.3.2. *Let $f(x) \in \mathbb{F}_q[x]$ and $a, b \in \mathbb{F}_q$, $b \neq 0$. Then the following statements are equivalent:*

(i) *$f(x)$ is a PP of $\mathbb{F}_q$,*

(ii) *$f(x)+a$ is a PP of $\mathbb{F}_q$,*

(iii) *$bf(x)$ is a PP of $\mathbb{F}_q$.*

Proof. The proof follows from Lemma 1.3.1, since we know that every linear polynomial over $\mathbb{F}_q$ is a PP of $\mathbb{F}_q$. □

1.4 Groups of Permutation Polynomials

Definition 1.4.1. Let n be a positive integer. The set of all one-to-one mappings, i.e. permutations, from the set $\{1, 2, ..., n\}$ onto $\{1, 2, ..., n\}$ forms a group under the composition. This group is called the *symmetric group* of *degree* n, and denoted by S_n.

Let $S = \{f(x)|\ f(x)$ is a PP of $\mathbb{F}_q\}$. Define an operation "." on the set S in such a way that $g(x).f(x) = h(x)$ whenever $f(g(x)) \equiv h(x) \bmod (x^q - x)$. Under this operation $(S, .)$ is a group and it is isomorphic to the symmetric group S_q.

Theorem 1.4.1. *For $q > 2$, S_q is generated by x^{q-2} and all (non-constant) linear polynomials over $\mathbb{F}_q$.*

Proof. Note that the polynomial $f_a(x) = -a^2[((x-a)^{q-2}+a^{-1})^{q-2}-a]^{q-2}$ represents the transposition $(0a)$, $a \in \mathbb{F}_q^*$. Since every permutation of $\mathbb{F}_q$ is a product of transpositions and that every transposition (bc) can be written as a product $(0b)(0c)(0b)$, we conclude the proof. □

Theorem 1.4.2. *If $q > 2$ and c is a fixed primitive element of $\mathbb{F}_q$, then S_q is generated by $cx, x+1$, and x^{q-2}.*

Proof. Let $a, b \in \mathbb{F}_q$. Then there exist $s, t \in \mathbb{Z}$ such that $a = c^s$ and $b = c^t$. Now, the Theorem follows from the identity $ax+b = (cx)^{s-t}.(x+1).(cx)^t$ and Theorem 1.4.1. □

Theorem 1.4.3. *Let*

$$S = \{D_k(x, a) \in \mathbb{F}_q[x]|\ (k, q^2 - 1) = 1\}$$

be the set of all Dickson Polynomials $D_k(x, a) \in \mathbb{F}_q[x]$ that are PPs over $\mathbb{F}_q$. Then S is closed under the composition of polynomials if and only if $a = 0, 1$ or -1.

Proof. Assume that $a \neq 0$ and S is closed under composition. Let $D_k(x, a)$ and $D_m(x, a)$ be two polynomials in S. Then their composition $D_k(D_m(x, a), a)$ is also

in S. Since from the choice of $D_k(x,a)$ and $D_m(x,a)$, $(k,q^2-1)=(m,q^2-1)=1$, we have $(km,q^2-1)=1$ and therefore, the polynomial $D_{km}(x,a)$ is also in S. But from (1.2),

$$deg(D_k(D_m(x,a),a)) = deg(D_{km}(x,a)),$$

which implies that

$$D_k(D_m(x,a),a) = D_{km}(x,a). \tag{1.4}$$

Using (1.3), one gets

$$\begin{aligned} D_{km}(y+\frac{a}{y},a) &= y^{km}+\frac{a^{km}}{y^{km}} \\ &= D_k\left(y^m+\frac{a^m}{y^m},a^m\right) \\ &= D_k\left(D_m\left(y+\frac{a}{y},a\right),a^m\right). \end{aligned}$$

Hence,

$$D_{km}(x,a) = D_k(D_m(x,a),a^m). \tag{1.5}$$

Now combining (1.4) and (1.5), we get

$$D_k(D_m(x,a),a) = D_k(D_m(x,a),a^m). \tag{1.6}$$

Since $D_m(x,a)$ is an onto function, we can write (1.6) as

$$D_k(x,a) = D_k(x,a^m).$$

And comparing the coefficient of x^{k-2} in these two polynomials, we conclude that $a^m=a$, and this holds for all m with $(m,q^2-1)=1$. Thus for $m=q-2$,

$$a^{q-2} = a^{-1} = a$$

so that $a=1$ or -1.

Now, conversely assume that $a=0,1$ or -1. Let $D_k(x,a)$ and $D_m(x,a)$ be two polynomials in S, so that $(k,q^2-1)=(m,q^2-1)=1$. We want to show that the composition $D_k(D_m(x,a),a)$ is also in S. First note that, for $a=0,1$ or -1,

$$D_k(D_m(x,a),a) = D_k(D_m(x,a),a^m)$$

and by (1.5)

$$D_k(D_m(x,a),a) = D_{km}(x,a).$$

Since $(km,q^2-1)=1$, $D_{km}(x,a)\in S$, therefore, $D_k(D_m(x,a),a)\in S$. □

CHAPTER 2

ENUMERATION OF PERMUTATION POLYNOMIALS

Lidl and Mullen listed a number of open problems related to PPs in [6], [7]. In this Chapter we will be dealing with one of these problems, namely finding the number of PPs of a given degree d.

2.1 An Upper Bound for the Number of Permutation Polynomials with Non-Maximal Degree

Recall that from (1.1) all PPs of a finite field $\mathbb{F}_q$ have degree $\leq q-2$. In [4] Konyagin and Pappalardi give an asymptotic bound for the number of PPs of degree less than $q-2$ and state that almost all PPs of $\mathbb{F}_q$ have degree $q-2$, according to the following Theorem. We will first present some notation. Let

$$N_q(d) = |\{\sigma \in S_q |\ deg(f_\sigma) = d\}|$$

and

$$N(q,m) = |\{\sigma \in S_q |\ deg(f_\sigma) < q-m\}|.$$

Theorem 2.1.1. *For $N(q,2)$, where $N(q,2) = |\{\sigma \in\ S_q |\ deg(f_\sigma) < q-2\}|$, we have*

$$|N(q,2) - (q-1)!| \leq \sqrt{\frac{2e}{\pi}} q^{\frac{q}{2}}.$$

Hence for $N_q(q-2)$, where $N_q(q-2)$ represents the number of PPs of $\mathbb{F}_q$ of degree $q-2$, we have a significantly large lower bound

$$N_q(q-2) \geq (q-1)!(q-1) - \sqrt{\frac{2e}{\pi}} q^{\frac{q}{2}}.$$

We have the following table for the values of $N(q,2)$, corresponding to the first eight prime powers.

q	2	3	4	5	7	8	9	11
$N(q,2)$	0	0	12	20	630	5368	42120	3634950
$(q-1)!$	1	2	6	24	720	5040	40320	3628800

Proof. Let S be a fixed subset of $\mathbb{F}_q$.

Define

$$N_S = |\{f | f : \mathbb{F}_q \to S, \text{ and } \sum_{c \in S} cf(c) = 0\}|.$$

From (1.1), one can easily see that, for a permutation $\sigma \in S_q$ the coefficient of x^{q-2} in $f_\sigma(x)$ is

$$-\sum_{c \in \mathbb{F}_q} c\sigma(c),$$

so that $deg(f_\sigma) < q-2$ if and only if

$$\sum_{c \in \mathbb{F}_q} c\sigma(c) = 0.$$

Therefore for $N(q,2)$ we have

$$N(q,2) = N_{\mathbb{F}_q} + \sum_{S \subsetneq \mathbb{F}_q} (-1)^{q-|S|} N_S = \sum_{S \subseteq \mathbb{F}_q} (-1)^{q-|S|} N_S. \tag{2.1}$$

Put $e_p(x) = e^{\frac{2\pi i x}{p}}$. Then from the properties of additive characters, it follows that

$$\sum_{a \in \mathbb{F}_q} e_p(Tr(ax)) = \begin{cases} q & \text{if } x = 0 \\ 0 & \text{if } x \neq 0. \end{cases}$$

Now using the identity

$$\frac{1}{q} \sum_{a \in \mathbb{F}_q} e_p \left(Tr(a \sum_{c \in \mathbb{F}_q} cf(c)) \right) = \begin{cases} 1 & \text{if } \sum_{c \in \mathbb{F}_q} cf(c) = 0 \\ 0 & \text{otherwise.} \end{cases}$$

we have

$$\begin{aligned} N_S &= \sum_{f:\mathbb{F}_q \to S} \left(\frac{1}{q} \sum_{a \in \mathbb{F}_q} e_p \left(Tr(a \sum_{c \in \mathbb{F}_q} cf(c)) \right) \right) \\ &= \frac{1}{q} \sum_{a \in \mathbb{F}_q} \left(\sum_{f:\mathbb{F}_q \to S} e_p \left(\sum_{c \in \mathbb{F}_q} Tr(acf(c)) \right) \right) \\ . &= \frac{1}{q} \sum_{a \in \mathbb{F}_q} \left(\prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(Tr(act)) \right) \\ &= \frac{|S|^q}{q} + \frac{1}{q} \sum_{a \in \mathbb{F}_q^*} \left(\prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(Tr(ct)) \right) \\ &= \frac{|S|^q}{q} + \frac{q-1}{q} \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(Tr(ct)). \end{aligned} \tag{2.2}$$

Combining (2.1) with (2.2), we obtain

$$N(q,2) - \sum_{S \subseteq \mathbb{F}_q} \frac{(-1)^{q-|S|}}{q} |S|^q = \frac{q-1}{q} \sum_{S \subseteq \mathbb{F}_q} (-1)^{q-|S|} \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(Tr(ct)).$$

We also note that

$$\begin{aligned} \sum_{S \subseteq \mathbb{F}_q} \frac{(-1)^{q-|S|}}{q} |S|^q &= \frac{1}{q} \left\{ q^q - \sum_{S \subsetneq \mathbb{F}_q} (-1)^{q-|S|} |S|^q \right\} \\ &= \frac{1}{q} q! \\ &= (q-1)!. \end{aligned}$$

Therefore,

$$N(q,2) - (q-1)! = \frac{q-1}{q} \sum_{S \subseteq \mathbb{F}_q} (-1)^{q-|S|} |S| \prod_{c \in \mathbb{F}_q^*} \sum_{t \in S} e_p(Tr(ct)).$$

Using the fact that

$$\sum_{t \in S} e_p(Tr(ct)) = -\sum_{t \notin S} e_p(Tr(ct)) \text{ for } c \in \mathbb{F}_q^*,$$

we consider two cases:

(i) If q is odd, then

$$\prod_{c \in \mathbb{F}_q^*} \left(-\sum_{t \in S} e_p(Tr(ct)) \right) = \prod_{c \in \mathbb{F}_q^*} \sum_{t \in S} e_p(Tr(ct)).$$

Also note that $|S|$ is even if and only if $q - |S|$ is odd, hence, for each subset S of $\mathbb{F}_q$

$$(-1)^{q-|S|} = -(-1)^{|S|}$$

$$\begin{aligned} N(q,2)-(q-1)! &= \frac{q-1}{2q}\sum_{S\subseteq\mathbb{F}_q}((-1)^{q-|S|}+(-1)^{|S|}(q-|S|))\prod_{c\in\ \mathbb{F}_q^*}\sum_{t\in\ S}e_p(Tr(ct)) \\ &= \frac{q-1}{2q}\sum_{S\subseteq\mathbb{F}_q}(-1)^{|S|}(q-2|S|)\prod_{c\in\ \mathbb{F}_q^*}\sum_{t\in\ S}e_p(Tr(ct)). \end{aligned} \tag{2.3}$$

(ii) If q is even, then

$$\prod_{c\in\ \mathbb{F}_q^*}\left(-\sum_{t\in\ S}e_p(Tr(ct))\right)=-\prod_{c\in\ \mathbb{F}_q^*}\sum_{t\in\ S}e_p(Tr(ct))$$

and $|S|$ is even if and only if $q-|S|$ is even. Hence,

$$(-1)^{q-|S|}=-(-1)^{|S|}.$$

Therefore

$$\begin{aligned} N(q,2)-(q-1)! &= \frac{q-1}{2q}\sum_{S\subseteq\mathbb{F}_q}((-1)^{|S|}-(-1)^{|S|}(q-|S|))\prod_{c\in\ \mathbb{F}_q^*}\sum_{t\in\ S}e_p(Tr(ct)) \\ &= \frac{q-1}{2q}\sum_{S\subseteq\mathbb{F}_q}(-1)^{|S|}(2|S|-q)\prod_{c\in\ \mathbb{F}_q^*}\sum_{t\in\ S}e_p(Tr(ct)). \end{aligned} \tag{2.4}$$

Now taking the absolute value of both sides in (2.3) and (2.4) , we get

$$|N(q,2)-(q-1)!|\leq\frac{q-1}{2q}\sum_{S\subseteq\mathbb{F}_q}|q-2|S||\prod_{c\in\ \mathbb{F}_q^*}\left|\sum_{t\in\ S}e_p(Tr(ct))\right|. \tag{2.5}$$

Note that the geometric mean is always less than or equal to the arithmetic mean, i.e.

$$(\prod_{k=1}^{n}|a_i^2|)^{\frac{1}{k}}\leq\frac{1}{k}\sum_{k=1}^{n}|a_i^2|,$$

or equivalently,

$$\begin{aligned} (\prod_{k=1}^{n}|a_i|)^{\frac{2}{k}} &\leq \frac{1}{k}\sum_{k=1}^{n}|a_i^2|, \\ (\prod_{k=1}^{n}|a_i|) &\leq (\frac{1}{k}\sum_{k=1}^{n}|a_i^2|)^{\frac{k}{2}}. \end{aligned}$$

Taking

$$a_i=|\sum_{t\in\ S}e_p(Tr(c_it))|,\ \text{for } i=1,...,q-1$$

we have

$$\prod_{c\in\ \mathbb{F}_q^*}\left|\sum_{t\in\ S}e_p(Tr(ct))\right|\leq\left(\frac{1}{q-1}\sum_{c\in\ \mathbb{F}_q^*}\left|\sum_{t\in\ S}e_p(Tr(ct))\right|^2\right)^{\frac{q-1}{2}}. \tag{2.6}$$

We also note that

$$\begin{aligned}
\sum_{c\in\ \mathbb{F}_q}\left|\sum_{t\in\ S} e_p(Tr(ct))\right|^2 &= \sum_{c\in\ \mathbb{F}_q}\left(\sum_{t\in\ S} e_p(Tr(ct))\right)\left(\overline{\sum_{t\in\ S} e_p(Tr(ct))}\right)\\
&= \sum_{c\in\ \mathbb{F}_q}\left(\sum_{t\in\ S} e_p(Tr(ct))\right)\left(\sum_{t\in\ S}\overline{e_p(Tr(ct))}\right)\\
&= \sum_{c\in\ \mathbb{F}_q}\sum_{t_1,t_2\in\ S} e_pTr(ct_1)\overline{e_pTr(ct_2)}\\
&= \sum_{c\in\ \mathbb{F}_q}\sum_{t_1,t_2\in\ S} e_p(Tr(ct_1-ct_2))\\
&= \sum_{t_1,t_2\in\ S}\sum_{c\in\ \mathbb{F}_q} e_p(Tr(c(t_1-t_2)))\\
&= q|S|, \qquad (2.7)
\end{aligned}$$

where we used the following identity in the last step:

$$\sum_{c\in\ \mathbb{F}_q} e_p(Tr(c(t_1-t_2))) = \begin{cases} q & \text{if } t_1 = t_2\\ 0 & \text{if } t_1 \neq t_2 \end{cases}$$

So, we have

$$\sum_{c\in\ \mathbb{F}_q^*}\left|\sum_{t\in\ S} e_p(Tr(ct))\right|^2 = (q-|S|)|S|.$$

Hence (2.6) can be written as

$$\prod_{c\in\ \mathbb{F}_q^*}\left|\sum_{t\in\ S} e_p(Tr(ct))\right| \leq \left(\frac{(q-|S|)|S|}{q-1}\right)^{\frac{q-1}{2}}. \qquad (2.8)$$

Combining (2.8) with (2.5), we obtain

$$|N(q,2)-(q-1)!| \leq \frac{q-1}{2q(q-1)^{\frac{q-1}{2}}}\sum_{S\subseteq\mathbb{F}_q}|q-2|S||\left((q-|S|)|S|\right)^{\frac{q-1}{2}}. \qquad (2.9)$$

Now our aim is to estimate the right-hand side of this inequality. First note that

$$\begin{aligned}
\sum_{S\subseteq\mathbb{F}_q} |q-2|S|| &= 2\sum_{S\subseteq\mathbb{F}_q, |S|\leq\frac{q}{2}} (q-2|S|) \\
&= 2\sum_{j=0}^{\lfloor\frac{q}{2}\rfloor} \binom{q}{j}(q-2j) \\
&= 2\left[\sum_{j=0}^{\lfloor\frac{q}{2}\rfloor} \binom{q}{j}(q-j) - \sum_{j=1}^{\lfloor\frac{q}{2}\rfloor} \binom{q}{j}(j)\right] \\
&= 2\left[\sum_{j=0}^{\lfloor\frac{q}{2}\rfloor} \frac{q!}{(q-j)!j!}(q-j) - \sum_{j=1}^{\lfloor\frac{q}{2}\rfloor} \frac{q!}{(q-j)!j!}j\right] \\
&= 2q\left[\sum_{j=0}^{\lfloor\frac{q}{2}\rfloor} \frac{(q-1)!}{(q-j-1)!j!} - \sum_{j=1}^{\lfloor\frac{q}{2}\rfloor} \frac{(q-1)!}{(q-j)!(j-1)!}\right] \\
&= 2q\left[\sum_{j=0}^{\lfloor\frac{q}{2}\rfloor} \binom{q-1}{j} - \sum_{j=1}^{\lfloor\frac{q}{2}\rfloor} \binom{q-1}{j-1}\right] \\
&= 2q\binom{q-1}{\lfloor\frac{q}{2}\rfloor}.
\end{aligned} \tag{2.10}$$

Using the inequality

$$\binom{2n}{n} \leq \sqrt{\frac{2}{\pi}}\frac{2^{2n}}{\sqrt{2n+\frac{1}{2}}}$$

we also have

$$\binom{q-1}{\lfloor\frac{q}{2}\rfloor} \leq \sqrt{\frac{2}{\pi}}\frac{2^{q-1}}{\sqrt{q-\frac{1}{2}}}.$$

Hence (2.10) can be written as

$$\sum_{S\subseteq\mathbb{F}_q} |q-2|S|| = 2q\binom{q-1}{\lfloor\frac{q}{2}\rfloor} \leq \sqrt{\frac{2}{\pi}}\frac{2^q q}{\sqrt{q-\frac{1}{2}}}. \tag{2.11}$$

On the other hand,

$$\begin{aligned}
((q-|S|)|S|)^{\frac{q-1}{2}} &\leq \left((q-\left\lfloor\frac{q}{2}\right\rfloor)\left\lfloor\frac{q}{2}\right\rfloor\right)^{\frac{q-1}{2}} \\
&= \left(\sqrt{(q-\left\lfloor\frac{q}{2}\right\rfloor)\left\lfloor\frac{q}{2}\right\rfloor}\right)^{q-1} \\
&\leq (\frac{q}{2})^{q-1}.
\end{aligned} \tag{2.12}$$

Inserting (2.11) and (2.12) in (2.9), we have

$$|N(q,2)-(q-1)!| \leq \left(\frac{q-1}{\sqrt{q-\frac{1}{2}\sqrt{q}}}\right)\sqrt{\frac{2}{\pi}}\left(\frac{q}{q-1}\right)^{\frac{q-1}{2}} q^{\frac{q}{2}}. \tag{2.13}$$

Considering the inequalities

$$\frac{q-1}{\sqrt{q-\frac{1}{2}\sqrt{q}}} < 1 \text{ and } \left(\frac{q}{q-1}\right)^{\frac{q-1}{2}} < \sqrt{e}$$

we obtain

$$|N(q,2)-(q-1)!| \leq \sqrt{\frac{2e}{\pi}} q^{\frac{q}{2}}.$$

□

Following their results in [4], Konyagin and Pappalardi extended their work obtaining in [5] an asymtotic bound for the number of PPs of degree not exceeding a fixed number $q-m-1$ on a finite field. Before giving the related Theorem, we present further notation.

Let $\sigma \in S_q$ with the representing polynomial

$$f_\sigma(x) = \sum_{i=1}^{q-2} a_i x^i.$$

Let $k_1, ..., k_d \in \mathbb{Z}$ with $1 \leq k_1 < ... < k_d \leq q-2$. Then define

$$N[k_1, ..., k_d] = |\{\sigma \in S_q | a_{k_i} = 0 \text{ for all } i = 1, ..., d\}|.$$

Theorem 2.1.2.

$$|N[k_1, ..., k_d] - \frac{q!}{q^d}| < (q(q-k_1-1))^{\frac{q}{2}} \left(1+\sqrt{\frac{1}{e}}\right)^q.$$

Proof. Recall that for a permutation $\sigma \in S_q$, the corresponding $f_\sigma(x)$ is given by

$$f_\sigma(x) = \sum_{c \in \mathbb{F}_q} \sigma(c)(1-(x-c)^{q-1}).$$

Therefore the coefficient of x^i in $f_\sigma(x)$ is

$$(-1)^{q-i}\binom{q-1}{i} \sum_{c \in \mathbb{F}_q} c^{q-1-i}\sigma(c). \tag{2.14}$$

But in $\mathbb{F}_q$,

$$\begin{aligned}\binom{q-1}{i} &= \frac{(q-1)...(q-i)}{i!} \\ &= \frac{(-1)^i i!}{i!} \\ &= (-1)^i\end{aligned}$$

for all $i = 1, ..., q-1$. So, (2.14) is equal to

$$(-1)^q \sum_{c \in \mathbb{F}_q} c^{q-1-i}\sigma(c) = -\sum_{c \in \mathbb{F}_q} c^{q-1-i}\sigma(c).$$

Therefore, the coefficients $a_{k_i} = 0$ for $i = 1, ..., d$ if and only if

$$\sum_{c \in \mathbb{F}_q} c^{q-k_i-1}\sigma(c) = 0, \ i = 1, ..., d.$$

Now define,

$$N_S[k_1, ..., k_d] = |\{f | f : \mathbb{F}_q \to S, \text{ and } \sum_{c \in \mathbb{F}_q} c^{q-k_i-1} f(c) = 0, \text{ for all } i = 1, ..., d\}|.$$

Then we can write

$$\begin{aligned} N[k_1, ..., k_d] &= N_{\mathbb{F}_q}[k_1, ..., k_d] + \sum_{S \subsetneq \mathbb{F}_q} (-1)^{q-|S|} N_S[k_1, ..., k_d]. \\ &= \sum_{S \subseteq \mathbb{F}_q} (-1)^{q-|S|} N_S[k_1, ..., k_d] \end{aligned} \tag{2.15}$$

Then

$$\begin{aligned} N_S[k_1, ..., k_d] &= \frac{1}{q^d} \sum_{f:\mathbb{F}_q \to S} \left(\sum_{a \in \mathbb{F}_q} e_p(Tr(\sum_{c \in \mathbb{F}_q} f(c) a c^{q-k_1-1})) ... \sum_{a \in \mathbb{F}_q} e_p(Tr(\sum_{c \in \mathbb{F}_q} f(c) a c^{q-k_d-1})) \right) \\ &= \frac{1}{q^d} \sum_{f:\mathbb{F}_q \to S} \sum_{(a_1,...,a_d) \in \mathbb{F}_q^d} e_p(Tr(\sum_{c \in \mathbb{F}_q} f(c) a_1 c^{q-k_1-1})) ... e_p(Tr(\sum_{c \in \mathbb{F}_q} f(c) a_d c^{q-k_d-1})) \\ &= \frac{1}{q^d} \sum_{f:\mathbb{F}_q \to S} \sum_{(a_1,...,a_d) \in \mathbb{F}_q^d} e_p(\sum_{c \in \mathbb{F}_q} Tr(f(c) a_1 c^{q-k_1-1})) ... e_p(\sum_{c \in \mathbb{F}_q} Tr(f(c) a_d c^{q-k_d-1})) \\ &= \frac{1}{q^d} \sum_{f:\mathbb{F}_q \to S} \sum_{(a_1,...,a_d) \in \mathbb{F}_q^d} e_p \left(\sum_{c \in \mathbb{F}_q} Tr(f(c) a_1 c^{q-k_1-1}) + ... + \sum_{c \in \mathbb{F}_q} Tr(f(c) a_d c^{q-k_d-1}) \right) \\ &= \frac{1}{q^d} \sum_{(a_1,...,a_d) \in \mathbb{F}_q^d} \sum_{f:\mathbb{F}_q \to S} e_p \left(\sum_{c \in \mathbb{F}_q} Tr \left(f(c) \sum_{i=1}^{d} a_i c^{q-k_i-1} \right) \right) \\ &= \frac{1}{q^d} \sum_{(a_1,...,a_d) \in \mathbb{F}_q^d} \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p \left(Tr \left(t \sum_{i=1}^{d} a_i c^{q-k_i-1} \right) \right) \\ &= \frac{|S|^q}{q^d} + \frac{1}{q^d} \sum_{(a_1,...,a_d) \in \mathbb{F}_q^d \setminus \{0\}} \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p \left(Tr \left(t \sum_{i=1}^{d} a_i c^{q-k_i-1} \right) \right). \end{aligned}$$

Let

$$R_S := \sum_{(a_1,...,a_d) \in \mathbb{F}_q^d \setminus \{0\}} \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p \left(Tr \left(t \sum_{i=1}^{d} a_i c^{q-k_i-1} \right) \right)$$

and

$$M := \max_{(a_1,...,a_d) \in \mathbb{F}_q^d \setminus \{0\}} \prod_{c \in \mathbb{F}_q} \left| \sum_{t \in S} e_p \left(Tr \left(t \sum_{i=1}^{d} a_i c^{q-k_i-1} \right) \right) \right|.$$

Then since $|\{(a_1,...,a_d) \in \mathbb{F}_q^d \backslash \{0\}\}| = q^d - 1$, we have

$$|R_S| \leq (q^d - 1)M,$$

and therefore

$$N_S[k_1,...,k_d] \leq \frac{|S|^q}{q^d} + \frac{q^d-1}{q^d}M. \tag{2.16}$$

We again use the fact that the geometric mean is always bounded by the arithmetic mean to get

$$\prod_{c\in\mathbb{F}_q} \left|\sum_{t\in S} e_p\left(Tr\left(t\sum_{i=1}^{d} a_i c^{q-k_i-1}\right)\right)\right| \leq \left(\frac{1}{q}\sum_{c\in\mathbb{F}_q}\left|\sum_{t\in S} e_p\left(Tr\left(t\sum_{i=1}^{d} a_i c^{q-k_i-1}\right)\right)\right|^2\right)^{\frac{q}{2}} \tag{2.17}$$

Consider the polynomial $p(x) = \sum_{i=1}^{d} a_i x^{q-k_i-1}$. Since $p(x)$ has degree $q-k_1-1$, for each $u \in \mathbb{F}_q$, the equation

$$p(x) = \sum_{i=1}^{d} a_i x^{q-k_i-1} = 0$$

has at most $q-k_1-1$ solutions in $\mathbb{F}_q$. Therefore

$$\sum_{c\in\mathbb{F}_q}\left|\sum_{t\in S} e_p\left(Tr\left(t\sum_{i=1}^{d} a_i c^{q-k_i-1}\right)\right)\right|^2 \leq \sum_{u\in\mathbb{F}_q}(q-k_1-1)\left|\sum_{t\in S} e_p(Tr(tu))\right|^2. \tag{2.18}$$

Now combining (2.18) with (2.17) we obtain

$$\begin{aligned}\prod_{c\in\mathbb{F}_q} \left|\sum_{t\in S} e_p\left(Tr\left(t\sum_{i=1}^{d} a_i c^{q-k_i-1}\right)\right)\right| &\leq \left(\frac{1}{q}\sum_{u\in\mathbb{F}_q}(q-k_1-1)\left|\sum_{t\in S} e_p(Tr(tu))\right|^2\right)^{\frac{q}{2}} \\ &= (|S||q-k_1-1|)^{\frac{q}{2}}\end{aligned}$$

where we used the identity

$$\sum_{c\in\mathbb{F}_q}\left|\sum_{t\in S} e_p(Tr(tc))\right|^2 = q|S|$$

in the last step. Then from the definition of M and (2.16), it follows that

$$N_S[k_1,...,k_d] \leq \frac{|S|^q}{q^d} + \frac{q^d-1}{q^d}(|q-k_1-1||S|)^{\frac{q}{2}}. \tag{2.19}$$

Now inserting (2.19) in (2.15), we obtain

$$\begin{aligned}N[k_1,...,k_d] &\leq \sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}\left(\frac{|S|^q}{q^d} + \frac{q^d-1}{q^d}(|q-k_1-1||S|)^{\frac{q}{2}}\right) \\ &= \sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}\frac{|S|^q}{q^d} + \sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}\frac{q^d-1}{q^d}(|q-k_1-1||S|)^{\frac{q}{2}}.\end{aligned} \tag{2.20}$$

Using the fact that

$$\sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}|S|^q = q!$$

(2.20) becomes

$$N[k_1,...,k_d] \leq \frac{q!}{q^d} + \sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}\frac{q^d-1}{q^d}(|q-k_1-1||S|)^{\frac{q}{2}}.$$

Therefore,

$$\begin{aligned}\left|N[k_1,...,k_d] - \frac{q!}{q^d}\right| &\leq \frac{q^d-1}{q^d}\sum_{S\subseteq\mathbb{F}_q}(|q-k_1-1||S|)^{\frac{q}{2}} \\ &< |q-k_1-1|^{\frac{q}{2}}\sum_{S\subseteq\mathbb{F}_q}|S|^{\frac{q}{2}} \\ &= (q-k_1-1)^{\frac{q}{2}}\sum_{n=0}^{q}\binom{q}{n}n^{\frac{q}{2}}. \qquad (2.21)\end{aligned}$$

Now, since $1+x<e^x$, for $x=\frac{n-q}{q}$ we have

$$\begin{aligned}1+\frac{n-q}{q} &\leq e^{\frac{n-q}{q}} \\ n &\leq qe^{\frac{n-q}{q}}. \qquad (2.22)\end{aligned}$$

Therefore, inserting (2.22) in (2.21),

$$\begin{aligned}\left|N[k_1,...,k_d] - \frac{q!}{q^d}\right| &\leq (q-k_1-1)^{\frac{q}{2}}\sum_{n=0}^{q}\binom{q}{n}(qe^{\frac{n-q}{q}})^{\frac{q}{2}} \\ &= ((q-k_1-1)q)^{\frac{q}{2}}\sum_{n=0}^{q}\binom{q}{n}\left(\sqrt{\frac{1}{e}}\right)^{q-n} \\ &= ((q-k_1-1)q)^{\frac{q}{2}}\left(1+\sqrt{\frac{1}{e}}\right)^{q}.\end{aligned}$$

□

Corollary 2.1.1. *For $N(q,m+1)$, we have $N(q,m+1)\approx\frac{q!}{q^m}$, if $m\leq\frac{q}{\log q}(\frac{1}{2}\log\log q - \log\log\log q)$ and q is large enough.*

Proof. Note that

$$N(q,m+1) = N[q-m-1,...,q-2].$$

Therefore in Theorem 2.1.2 taking $k_1 = q-m-1$, we have

$$\begin{aligned}\left|N(q,m+1) - \frac{q!}{q^m}\right| &< (mq)^{\frac{q}{2}}(1+\sqrt{\frac{1}{e}})^q \\ &< (mq)^{\frac{q}{2}}2^q \qquad (2.23)\end{aligned}$$

Now the Corollary follows using the Stirling formula which states that

$$\lim_{q\to\infty}\frac{q!}{\sqrt{2\pi q}(\frac{q}{e})^q} = 1$$

for an estimation of the right-hand side of (2.23). □

2.2 The Number of Permutation Polynomials with Non-Maximal Degree

Let σ be a permutation of the elements of $\mathbb{F}_q$. Define the set

$$S_\sigma = \{c \in \mathbb{F}_q | \sigma(c) \neq c\}$$

i.e. S_σ is the set of all elements of $\mathbb{F}_q$ that are not fixed by σ. Note that the roots of the polynomial $f_\sigma(x) - x$ are all elements of $\mathbb{F}_q$ that are not in S_σ. Hence, if $\sigma \neq id$, so that $f_\sigma(x) \not\equiv x$, then $deg(f_\sigma(x) - x) = deg(f_\sigma)$ and hence $deg(f_\sigma)$ is at least $q - |S_\sigma|$. Recall that we have $deg(f_\sigma) \leq q - 2$. So if $\sigma \neq id$, we get

$$q - |S_\sigma| \leq deg(f_\sigma) \leq q - 2.$$

In particular, we conclude that all transpositions in $\mathbb{F}_q$ correspond to PPs of degree $q - 2$, compared with Theorem 1.4.1. Now we recall that a cycle $(a_1\ a_2 ... a_k) \in S_n$ is the permutation which sends a_k to a_1 and a_i to a_{i+1} for $1 \leq i \leq k - 1$, fixing all the elements j, where $1 \leq j \leq n$, $j \neq a_i$ for $i = 1, ..., k$. The length of a cycle is the number of integers which appear in it and a cycle of length k is called a *k-cycle*.

Let σ be a permutation in S_n. Then the *conjugacy class* of σ is defined by

$$C(\sigma) = \{\tau\sigma\tau^{-1} \mid \tau \in S_n\}.$$

Proposition 2.2.1. *Let σ and τ be two permutations in S_n. Suppose σ has the cycle decomposition*

$$(a_1\ a_2 ... a_{k_1})\ (b_1\ b_2 ... b_{k_2}) ....$$

Then $\tau\sigma\tau^{-1}$ has the cycle decomposition

$$(\tau(a_1)\ \tau(a_2) ... \tau(a_{k_1}))\ (\tau(b_1)\ \tau(b_2) ... \tau(b_{k_2})) ....$$

Proof. The proof follows from the observation that if $\sigma(i) = j$, then

$$\tau\sigma\tau^{-1}(\tau(i)) = \tau(j).$$

Therefore if (ij) is an ordered pair in σ, then $(\sigma(i)\sigma(j))$ is an ordered pair in $\tau\sigma\tau^{-1}$. □

We therefore have by Proposition 2.2.1 that, if σ_1 and σ_2 are two conjugate permutations, then their cycle decompositions have the same structure, i.e. the lengths of the cycles in both permutations are the same. Conversely, as easily can be seen, if two permutations σ_1 and σ_2 have the same cycle structure then they are conjugate. Hence the conjugacy classes of permutations in S_n form a partition of S_n.

Now, let ζ be a conjugacy class in S_n. Then, fixing q and m we define a function

$$N_\zeta(q,m) = |\{\sigma \in \zeta \ | deg(f_\sigma) < q - m\}|$$

on the set of conjugacy classes of permutations in S_n. In 1968 Wells (see [16]) gave the formula for the number $N_\zeta(q,2)$ for the conjugacy class ζ of 3-cycles which we denote by $\zeta = [3]$. Later in 2002, Malvenuto and Pappalardi generalized this result to some more conjugacy classes (see [9]). In this section we will present these results of Wells, Malvenuto and Pappalardi.

Theorem 2.2.1. *If $q > 3$, then the number of 3-cycle permutations σ of $\mathbb{F}_q$ with $deg(f_\sigma) \leq q-3$ is*

$$N_{[3]}(q,2) = \begin{cases} \frac{1}{3}q(q-1) & \text{if } q \equiv 0 \bmod 3 \\ \frac{2}{3}q(q-1) & \text{if } q \equiv 1 \bmod 3 \\ 0 & \text{if } q \equiv 2 \bmod 3 \end{cases}$$

Proof. Let $\sigma = (a\ b\ c)$ be a 3-cycle in S_q. Then, σ can be represented by

$$f_\sigma(x) = x + (a-b)(x-a)^{q-1} + (b-c)(x-b)^{q-1} + (c-a)(x-c)^{q-1}.$$

Note that the coefficient of x^{q-2} in $f_\sigma(x)$ is

$$a_{q-2} = a(a-b) + b(b-c) + c(c-a).$$

Hence, the polynomial $f_\sigma(x)$ is of degree $< q-2$ if and only if $a_{q-2} = 0$ or a is a solution of the equation

$$x^2 - (b+c)x + b^2 + c^2 - bc = 0. \tag{2.24}$$

The discriminant of this equation is

$$\Delta = -3(b-c)^2, \tag{2.25}$$

so that the system has a solution if and only if -3 is a square element in $\mathbb{F}_q$. We will continue the proof in two cases. First assume that q is odd. Then the characteristic p is odd, and -3 is a square element in $\mathbb{F}_p$ if and only if $\left(\frac{-3}{p}\right) = 1$, where $\left(\frac{a}{p}\right)$ is the Legendre symbol. Now, since p is an odd number, we have two subcases:

(i) If $p \equiv 1 \bmod 4$, then from the quadratic reciprocity law, it follows that

$$\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right).$$

Therefore,

$$\left(\frac{-3}{p}\right) = 1 \text{ if and only if } \left(\frac{p}{3}\right) = 1 \text{ if and only if } p \equiv 1 \bmod 3.$$

(ii) If $p \equiv 3 \bmod 4$, then again from the quadratic reciprocity law, it follows that

$$\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = -\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right).$$

giving the same result

$$\left(\frac{p}{3}\right) = 1 \text{ if and only if } p \equiv 1 \bmod 3.$$

Clearly, if $p \equiv 0 \bmod 3$, then $\left(\frac{-3}{p}\right) = 1$, so by the reasoning in (i) and (ii), we conclude that the only case that $\left(\frac{-3}{p}\right) = -1$ occurs when $p \equiv 2 \bmod 3$.

Here, we also note that, if -3 is a square element of $\mathbb{F}_p$, then it is a square element in $\mathbb{F}_{p^k}$ for any k. And if -3 is not a square element in $\mathbb{F}_p$, then it is a square element in $\mathbb{F}_{p^k}$ if and only if k is even.

Finally, we can say that -3 is not a square element of $\mathbb{F}_q$, where $q = p^k$, if and only if $p \equiv 2 \bmod 3$ and k is odd, where the latter condition is equivalent to $q \equiv 2 \bmod 3$. Therefore, there is no 3-cycle over $\mathbb{F}_q$ that gives a permutation polynomial of $< q-2$, if q is odd and $q \equiv 2 \bmod 3$.

Now if $p \equiv 1 \bmod 3$, hence $q \equiv 1 \bmod 3$, the solutions of (2.24) are

$$x_{1,2} = \frac{1}{2}(b + c \mp \sqrt{-3}(b - c)).$$

So for every $q(q-1)$ choices of b and c, we have two values for a and since permuting the elements in a cycle does not change the permutation, we have $\frac{1}{3}2q(q-1)$ 3-cycles that give a PP of degree $< q-2$, if q is odd and $q \equiv 1 \bmod 3$. And lastly, if $q \equiv 0 \bmod 3$ then $\Delta = 0$ in (2.25), so for every $q(q-1)$ choices of b and c, a is uniquely determined, so we have $\frac{1}{3}q(q-1)$ 3-cycles that give a PP of degree $< q-2$, if q is odd and $q \equiv 0 \bmod 3$.

Now assume that q is even. Then the equation (2.24) can be written as

$$(x + b)(x + c) = (b + c)^2. \tag{2.26}$$

Setting $d = b+c$ and $y = d^{-1}(x+b)$, the last equation can be converted to $y^2+y+1 = 0$. The polynomial $y^2 + y + 1$ is irreducible over $\mathbb{F}_{2^n}$, that is, the system in (2.26) has no solution if and only if n is odd. But in this case $q = 2^n$ implies $q \equiv 2 \bmod 3$. The only remaining case is $q = 2^n$ when n is even. In this case $q \equiv 1 \bmod 3$ and for the $q(q-1)$ choices of b and c the system in (2.26) has two solutions in $\mathbb{F}_q$, therefore there are $\frac{1}{3}2q(q-1)$ 3-cycles that give a PP of degree $< q-2$, if q is even and $q \equiv 1 \bmod 3$. □

Let σ be a permutation of the elements of $\mathbb{F}_q$ that is represented by the PP $f_\sigma(x) = a_{q-2}x^{q-2}+a_{q-1}x^{q-1}+\ldots+a_0 \in \mathbb{F}_q[x]$. Then as we know from Chapter 1, the polynomial

$f_\sigma(x)$ can be written as

$$\begin{aligned} f_\sigma(x) &= \sum_{c\in\mathbb{F}_q}\sigma(c)(1-(x-c)^{q-1}) \\ &= \sum_{c\in\mathbb{F}_q}\sigma(c) - \sum_{c\in\mathbb{F}_q}\sigma(c)(x-c)^{q-1} \\ &= -\sum_{c\in\mathbb{F}_q}\sigma(c)\left(x^{q-1}+\binom{q-1}{1}x^{q-2}(-c)+\ldots+\binom{q-1}{q-1}x^0(-c)\right). \end{aligned}$$

Therefore, when $q>3$, the coefficient of x^{q-2} in $f_\sigma(x)$ is

$$\begin{aligned} a_{q-2} &= -\sum_{c\in\mathbb{F}_q}\sigma(c)c \\ &= \sum_{c\in\mathbb{F}_q}(c-\sigma(c))c \\ &= \sum_{c\in S_\sigma}(c-\sigma(c))c. \end{aligned} \tag{2.27}$$

Let $[l_1,\ldots,l_k]$ denote the conjugacy class of permutations that are products of cycles of length $l_1,\ldots,l_k$. Now if

$$\sigma=(c_{1,1},\ldots,c_{1,l_1})(c_{2,1},\ldots,c_{2,l_2}),\ldots,(c_{k,1},\ldots,c_{k,l_k})$$

then according to (2.27) the coefficient of x^{q-2} in $f_\sigma(x)$ is

$$a_{q-2}=\sum_{j=1}^{k}\sum_{i=1}^{l_j}(c_{j,i}-c_{j,i+1})c_{j,i}.$$

In what follows $(m_1,m_2,\ldots,m_t)$ will denote the elements of the conjugacy class $\zeta=(m_1,m_2,\ldots,m_t)$ which are the products of m_1 cycles of lenght 1, m_2 cycles of lenght 2,..., and m_t cycles of lenght t, where $m_1+2m_2+\ldots+tm_t=q$. Then we will have

$$|\zeta|=\frac{q!}{m_1!1^{m_1}m_2!2^{m_2}\ldots m_t!t^{m_t}}.$$

Now for the conjugacy class $\zeta=[l_1,\ldots,l_k]$, we define a polynomial A_ζ in c variables, where $c=l_1+\ldots+l_k$, as follows

$$A_{\zeta(x_1,\ldots,x_c)}=\sum_{i=1,i\notin\{l_1,l_1+l_2,\ldots,c\}}^{c}(x_i-x_{i+1})x_i+\sum_{i=1}^{k}(x_{l_1+\ldots+l_i}-x_{l_1+\ldots+l_{i-1}+1})x_{l_1+\ldots+l_i}$$

Then every permutation counted by $N_\zeta(q,2)$ is an element of $\mathbb{F}_q$ that is a root of the polynomial A_ζ. Since shifting the elements in a cycle or interchanging different cycles of the same length gives the same permutation, we have

$$N_\zeta(q,2)=\frac{|x=(x_1,\ldots,x_c)\in\mathbb{F}_q^c, x_i\neq x_j \text{ for } i\neq j \text{ and } A_\zeta(x)=0|}{m_2!2^{m_2}\ldots m_t!t^{m_t}}.$$

Now, as an application of the arguments above, we consider the conjugacy class $\zeta=[2,2]$, see [9].

Theorem 2.2.2. *Suppose q is odd and $q > 3$. Then*

$$N_{[2,2]}(q,2) = \frac{1}{8}q(q-1)(q-4)(1+\eta(-1)),$$

and if q is even, then

$$N_{[2,2]}(2^n,2) = \frac{1}{8}2^n(2^n-1)(2^n-2).$$

Proof. Let $\sigma = (ab)(cd)$ be a permutation that is represented by a PP of degree $< q-2$ in $\mathbb{F}_q[x]$. Then from (2.27) we get

$$\begin{aligned} (a-b)b + (b-a)b + (c-d)c + (d-c)d &= 0 \\ (a-b)^2 + (c-d)^2 &= 0. \end{aligned} \tag{2.28}$$

Note that this equation has a solution if and only if -1 is a square element in $\mathbb{F}_q$. First assume that q is an odd prime power. Then for the $q(q-1)$ fixed choices (a_0, b_0) for (a,b), we have

$$\begin{aligned} (c-d)^2 &= -(a_0-b_0)^2, \\ c &= d \mp \sqrt{-1}(a_0-b_0). \end{aligned}$$

Now for the choice of $d \in \mathbb{F}_q \backslash \{a_0, b_0, a_0 \mp \sqrt{-1}(a_0-b_0), b_0 \mp \sqrt{-1}(a_0-b_0)\}$, we have exactly 2 values for c. And if

$$d = a_0 \mp \sqrt{-1}(a_0-b_0) \text{ or } d = b_0 \mp \sqrt{-1}(a_0-b_0),$$

then, c is uniquely determined. Hence, we have

$$2q(q-1)(q-6) + 4q(q-1) = 2q(q-1)(q-4)$$

solutions for the equation (2.29). But, since permuting the elements in 2-cycles or interchanging the cycles do not give a different permutation,

$$\begin{aligned} N_{[2,2]}(q,2) &= \frac{1}{2.2.2}2q(q-1)(q-4) \\ &= \frac{1}{4}q(q-1)(q-4) \\ &= \frac{1}{8}q(q-1)(q-4)(1+\eta(-1)), \end{aligned}$$

where the last identity comes from the necessity that for (2.28) to have a solution, -1 should be a square element in $\mathbb{F}_q$.

Now if q is even, that is $q = 2^n$ for some integer n, the equation

$$(a-b)^2 + (c-d)^2 = 0$$

in (2.28) becomes

$$\begin{aligned} a^2+b^2+c^2+d^2 &= 0 \\ (a+b+c+d)^2 &= 0 \\ a+b+c+d &= 0. \end{aligned}$$

$$d = a+b+c.$$

and once the $q, q-1, q-2$ choices of a, b and c respectively are made, d is uniquely determined. Then with the same argument as before,

$$N_{[2,2]}(2^n, 2) = \frac{1}{8}2^n(2^n-1)(2^n-2).$$

□

2.3 The Number of Permutation Polynomials of a Given Degree

In his paper [2], Das gives a formula for the number of PPs of degree d by relating it to the number of solutions of a system of linear equations.

Definition 2.3.1. Let $A = (a_{ij})$, $i, j = 1, ..., n$, be an $n \times n$ matrix. The *permanent* of A is defined by

$$per(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)}.$$

where S_n is, as usual, the symmetric group of degree n.

Definition 2.3.2. Let $A = (a_{ij})$ be an $n \times n$ matrix. Then A is called a *Vandermonde matrix* and denoted by $A = Vand(z_1, z_2, \ldots, z_n)$ if $a_{ij} = z_j^{i-1}$ for $i, j = 1, 2, \ldots, n$.

Note that, in this section we will just consider the PPs with zero constant term. Now let $f(x) = a_{q-2}x^{q-2} + a_{q-1}x^{q-1} + ... + a_1x$ be in $\mathbb{F}_q[x]$ and $w \in \mathbb{F}_q$ be a primitive element so that the value set of f can be written as

$$V_f = \{f(0), f(1), f(w), ..., f(w^{q-2})\}.$$

Define the matrix $W = (w^{(i-1)(j-1)}) = Vand(1, w, ..., w^{q-2})$, $i, j = 1, ..., q-1$.
Considering the matrices

$$a = (0\ a_1\ a_2\ ...\ a_{q-2})^T \text{ and } v = (f(1)\ f(w)\ f(w^2)\ ...\ f(w^{q-2}))^T$$

we have

$$Wa = v,$$

or

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & \dots & w^{q-2} \\ 1 & w^2 & w^4 & \dots & w^{2(q-2)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w^{q-2} & w^{2(q-2)} & \dots & w^{(q-2)(q-2)} \end{pmatrix} \begin{pmatrix} 0 \\ a_1 \\ a_2 \\ \vdots \\ a_{q-2} \end{pmatrix} = \begin{pmatrix} a_1 + \ldots + a_{q-2} \\ a_1 w + \ldots + a_{q-2} w^{q-2} \\ a_1 w^2 + \ldots + a_{q-2} w^{2(q-2)} \\ \vdots \\ a_1 w^{q-2} + \ldots + a_{q-2} w^{(q-2)(q-2)} \end{pmatrix}.$$

Since W is an invertible (Vandermonde) matrix , we have

$$a = W^{-1} v.$$

If f is a PP of $\mathbb{F}_q$, then $v = P(1\ w\ w^2\ ...\ w^{q-2})^T$ where P denotes a permutation of the rows of v. Therefore

$$a = W^{-1} P(1\ w\ w^2\ ...\ w^{q-2})^T,$$

that is

$$\begin{pmatrix} 0 \\ a_1 \\ a_2 \\ \vdots \\ a_{q-2} \end{pmatrix} = \frac{1}{q-1} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w^{q-2} & w^{2(q-2)} & \dots & w^{(q-2)(q-2)} \\ 1 & w^{q-3} & w^{2(q-3)} & \dots & w^{(q-2)(q-3)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w & w^2 & \dots & w^{q-2} \end{pmatrix} P \begin{pmatrix} 1 \\ w \\ w_2 \\ \vdots \\ w_{q-2} \end{pmatrix}. \quad (2.29)$$

Let $\overline{N_q}(d)$ denote the number of permutation polynomials $f \in \mathbb{F}_q[x]$ with $deg(f) = d$ and $f(0) = 0$. Then we have the following theorem.

Theorem 2.3.1. *$\overline{N_q}(d)$ is equal to the number of solutions in $\mathbb{F}_q^{q-1}$ of the system of the equations*

$$\begin{aligned} x_1 + w^{q-d-1} x_2 + w^{2(q-d-1)} x_3 + \ldots + w^{(q-2)(q-d-1)} x_{q-1} &\neq 0 \\ x_1 + w^{q-d-2} x_2 + w^{2(q-d-2)} x_3 + \ldots + w^{(q-2)(q-d-2)} x_{q-1} &= 0 \\ &\vdots \\ x_1 + w x_2 + w^2 x_3 + \ldots + w^{q-2} x_{q-1} &= 0 \end{aligned} \quad (2.30)$$

with $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$, $i, j = 1, \ldots, q-1$.

Proof. Let $f(x) = a_{q-2}x^{q-2} + a_{q-1}x^{q-1} + \ldots + a_1 x \in \mathbb{F}_q[x]$ be a PP of $\mathbb{F}_q$. Then, $deg(f) = d$ if and only if $a_d \neq 0$ and $a_{d+1} = a_{d+2} = \ldots = 0$. From (2.29), we have the

following equations

$$\begin{aligned} a_d &= x_1 + w^{q-d-1}x_2 + w^{2(q-d-1)}x_3 + \ldots + w^{(q-2)(q-d-1)}x_{q-1} \\ a_{d+1} &= x_1 + w^{q-d-2}x_2 + w^{2(q-d-2)}x_3 + \ldots + w^{(q-2)(q-d-2)}x_{q-1} \\ &\vdots \\ a_{q-2} &= x_1 + wx_2 + \ldots + w^{q-2}x_{q-2} \end{aligned}$$

with $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$, $i, j = 1, \ldots, q-1$. Since every $q-1$ tuple $(x_1 \ \ldots \ x_{q-1})$ that is a solution of the system (2.30) gives a permutation polynomial of degree d in $\mathbb{F}_q[x]$, the Theorem follows. □

Corollary 2.3.1. *For the prime power q, we have*

$$\overline{N_q}(q-2) = (q-1)! - \#\,(x_1 + wx_2 + w^2x_3 + \ldots + w^{q-2}x_{q-1} = 0),$$

where # represents the number of solutions in $\mathbb{F}_q^{q-1}$ of the corresponding equation with $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$.
In particular, for a prime number p, we have

$$\overline{N_p}(p-2) = (p-1)! - \#\,(x_1 + 2x_2 + 3x_3 + \ldots + (p-1)x_{p-1} \equiv 0 \bmod p)$$

with $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$.

Proof. From Theorem 2.3.1, we have

$$\overline{N_q}(q-2) = \#\,(x_1 + wx_2 + w^2x_3 + \ldots + w^{q-2}x_{q-1} \neq 0).$$

But note that, we have in total $(q-1)!$ tuples $(x_1\ x_2\ \ldots\ x_{q-1})$ in $\mathbb{F}_q$ with $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$, so the result follows. □

Corollary 2.3.2. *Let $E_q(d)$ be the number of solutions in $\mathbb{F}_q$ of the system of equations*

$$\begin{aligned} x_1 + w^{q-d-1}x_2 + w^{2(q-d-1)}x_3 + \ldots + w^{(q-2)(q-d-1)}x_{q-1} &= 0 \\ x_1 + w^{q-d-2}x_2 + w^{2(q-d-2)}x_3 + \ldots + w^{(q-2)(q-d-2)}x_{q-1} &= 0 \\ &\vdots \\ x_1 + wx_2 + w^2x_3 + \ldots + w^{q-2}x_{q-1} &= 0 \end{aligned} \tag{2.31}$$

with $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$, $i, j = 1, \ldots, q-1$. Then,

$$\overline{N_q}(d) = (q-1)! - \overline{N_q}(q-2) - \overline{N_q}(q-3) - \ldots - \overline{N_q}(d+1) - E_q(d)$$

Now our aim is to give a formula for the number $\overline{N_p}(p-2)$. For this purpose, by Corollary 2.3.1, it is sufficient to find a formula for $\#\ (x_1+2x_2+3x_3+\ldots+(p-1)x_{p-1} \equiv 0 \bmod p)$.

Theorem 2.3.2. *Let $A = Vand(x, \ldots, x^{p-1})$ and $per(A) = \sum c_i x^i$. Then,*

$$\#\ (x_1 + 2x_2 + 3x_3 + \ldots + (p-1)x_{p-1} \equiv 0 \bmod p) = \sum_{i:p|i} c_i,$$

where the sum is over all those coefficients for which the exponent of x is divisible by p. Therefore,

$$\overline{N_p}(p-2) = (p-1)! - \sum_{i:p|i} c_i.$$

Proof. Since $A = Vand(x, \ldots, x^{p-1})$, i.e. $A = (x^{i-1}j)_{i,j=1,\ldots,p-1}$, we can write A explicitly as

$$A = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ x & x^2 & x^3 & \ldots & x^{p-1} \\ x^2 & x^4 & x^6 & \ldots & x^{2(p-1)} \\ \vdots & & & & \\ x^{p-2} & x^{2(p-2)} & x^{3(p-2)} & \ldots & x^{(p-1)(p-2)} \end{pmatrix}.$$

Define the matrix B by

$$B = \begin{pmatrix} x & x^2 & x^3 & \ldots & x^{p-1} \\ x^2 & x^4 & x^6 & \ldots & x^{2(p-1)} \\ x^3 & x^6 & x^9 & \ldots & x^{3(p-1)} \\ \vdots & & & & \\ x^{p-1} & x^{2(p-1)} & x^{3(p-1)} & \ldots & x^{(p-1)(p-1)} \end{pmatrix}.$$

Then it is easily seen that

$$\begin{aligned} per(B) &= xx^2x^3 \ldots x^{p-1} per(A) \\ &= x^{\frac{p(p-1)}{2}} per(A). \end{aligned} \tag{2.32}$$

Now, if x^n is an element in the expansion of $per(B)$, then $n = i_1 + 2i_2 + \ldots + (p-1)i_{p-1}$ for some $i_1, i_2, \ldots, i_{p-1} \in \mathbb{F}_q^*$ with $i_k \neq i_l$ for $k \neq l$. Therefore every term x^n in the expansion of $perB$ gives rise to a solution of the equation $x_1 + 2x_2 + 3x_3 + \ldots + (p-1)x_{p-1} \equiv 0 \bmod p$ such that $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$, and vice versa. But since p is a prime number, from (2.32) we observe that all terms x^n in $per(B)$, where n is divisible by p, come from the terms in $per(A)$ whose exponents are also divisible by p. □

Example 2.3.1. Now using Theorem 2.3.2, we will compute the number of PPs of degree 3, with zero constant term, in $\mathbb{F}_5[x]$. Let $A = Vand(x, x^2, x^3, x^4)$. Then

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ x & x^2 & x^3 & x^4 \\ x^2 & x^4 & x^6 & x^8 \\ x^3 & x^6 & x^9 & x^{12} \end{pmatrix}.$$

So, we have

$$per(A) = x^{20} + 3x^{19} + x^{18} + 4x^{17} + 2x^{16} + 2x^{15} + 2x^{14} + 4x^{13} + x^{12} + 3x^{11} + x^{10}.$$

Note that the coefficients of x^{20}, x^{15}, x^{10} are $1, 2, 1$, respectively, in per(A). Therefore

$$\#(x_1 + 2x_2 + 3x_3 + 4x_4 \equiv 0 \bmod 5) = 1 + 2 + 1 = 4.$$

Now, we conclude that the number of PPs of degree 3 in $\mathbb{F}_5[x]$ with constant term zero is

$$\overline{N_5}(3) = 4! - 4 = 20.$$

Remark 2.3.1. We would like to remark here that, if the condition $f(0) = 0$ is discarded, then we will have $5.20 = 100$ PPs of degree 3 in $\mathbb{F}_5[x]$. Also from the Table in Theorem 2.1.1, we know that there are 20 PPs of degree less than 3 in $\mathbb{F}_5[x]$. Adding these two values, we find that there are 120 PPs in $\mathbb{F}_5[x]$, in total, as is expected.

Remark 2.3.2. In the Example above, we found that there are 20 PPs of degree 3, with zero constant term expecting that there is $\frac{20}{4.5} = 1$ normalized PP of degree 3 in $\mathbb{F}_5[x]$. From the Table of Dickson's list of normalized PPs , we see that there is exactly one PP, namely x^3, in $\mathbb{F}_5[x]$, which is in accordence with our expectation. (If f is a normalized PP of $\mathbb{F}_q$, then taking the composition $af(x+b)+c$ with $a, b, c \in \mathbb{F}_q$, $a \neq 0$, we obtain $q(q-1)$ PPs with zero constant term corresponding to the $(q-1)$ choices of a and q choices of b.)

Theorem 2.3.3. *Let*

$$A = Vand(z_1 z_2 \dots z_n, z_1^2 z_2^{2^2} \dots z_n^{2^n}, \dots, z_1^{p-1} z_2^{(p-1)^2} \dots z_n^{(p-1)^n}),$$

where $1 \leq n \leq p-2$. *Let* $per(A) = \sum c_{i_1 i_2 \dots i_n} z_1^{i_1} z_2^{i_2} \dots z_n^{i_n}$. *Then the number of solutions in* $\mathbb{F}_q$ *of the system of equations*

$$\begin{aligned} x_1 + 2^n x_2 + 3^n x_3 + \dots + (p-1)^n x_{p-1} &= 0 \\ x_1 + 2^{n-1} x_2 + 3^{n-1} x_3 + \dots + (p-1)^{n-1} x_{p-1} &= 0 \\ &\vdots \\ x_1 + 2x_2 + 3x_3 + \dots + (p-1) x_{p-1} &= 0 \end{aligned}$$

with $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j, i, j = 1, \ldots, p-1$, is equal to $\sum_{p|i_1,\ldots,p|i_n} c_{i_1 i_2 \ldots i_n}$ where the sum is over all coefficients $c_{i_1 i_2 \ldots i_n}$ for which p divides the exponent i_k of each z_k.

Proof. The proof follows by a similar argument to that used in the proof of Theorem 2.3.2. □

Example 2.3.2. Now, suppose we want to find out the number of PPs of degree 2, with zero constant term, in $\mathbb{F}_5[x]$. From Corollary 2.3.2 we have

$$\overline{N_5}(2) = (5-1)! - \overline{N_5}(3) - E_5(2), \tag{2.33}$$

where $E_5(2)$ is the number of solutions in $\mathbb{F}_5$ of the system of equations

$$\begin{aligned} x_1 + w^2 x_2 + w^{2.2} x_3 + w^{3.2} x_4 &= 0 \\ x_1 + w x_2 + w^2 x_3 + w^3 x_4 &= 0 \end{aligned}$$

with $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$. Since we are in a prime field, this system of equations is equivalent to the system

$$\begin{aligned} x_1 + 2^2 x_2 + 3^2 x_3 + 4^2 x^4 &= 0 \\ x_1 + 2x_2 + 3x_3 + 4x_4 &= 0. \end{aligned}$$

Now in Theorem 2.3.3, let

$$A = Vand(z_1 z_2, z_1^2 z_2^{2^2}, z_1^3 z_2^{3^2}, z_1^4 z_2^{4^2})$$

and

$$per(A) = \sum ci_1 i_2 z_1^{i_1} z_2^{i_2}.$$

Then,

$$E_5(2) = \sum_{5|i_1, 5|i_2} c_{i_1 i_2}.$$

Writing $per(A)$ explicitly, we have all the terms $z_1^{20} z_2^{70}, 2z_1^{15} z_2^{45}, z_1^{10} z_2^{20}$ in which the exponents of both z_1 and z_2 are divisible by 5. So that

$$E_5(2) = 1 + 2 + 1 = 4.$$

Also from the previous example we know that $N_5(3) = 20$. Combining these results in (2.33), we get

$$\overline{N_5}(2) = 24 - 20 - 4 = 0.$$

Remark 2.3.3. The result in the Example 2.3.2 agrees with the Table in Theorem 2.1.1, since we know that there exist 20 PPs of degree less than 3 in $\mathbb{F}_5[x]$ and we know that all linear polynomials are PPs, and there are already 20 of them in $\mathbb{F}_5[x]$.

CHAPTER 3

SOME NEW CLASSES OF PERMUTATION POLYNOMIALS

In this Chapter we will present some new classes of PPs.

3.1 Permutation Polynomials of the form $x^r f(x^{\frac{q-1}{s}})$

Let s be a divisor of $q-1$. In this section, following [14], we present a criterion for the polynomials of the form $x^r f(x^{\frac{q-1}{s}})$ to be PPs of $\mathbb{F}_q$. First we introduce some notation. Let g be a primitive element of $\mathbb{F}_q$, and $\xi = g^{\frac{q-1}{s}}$ be a primitive s-th root of unity $\in \mathbb{F}_q$. Now for all $a \in \mathbb{F}_q^*$, we put

$$E_g(a) = \overline{k} \bmod (q-1),$$

where $a = g^k$ and $\overline{k}$ denotes the least residue modulo $(q-1)$ of k.
Let

$$\psi(a) = E_g(a) \bmod s.$$

Then, we have the following identities:

$$\begin{aligned} E_g(a^x) &= xE_g(a), \\ E_g(ab) &= E_g(a) + E_g(b), \\ g^{E_g(a)} &= a. \end{aligned} \tag{3.1}$$

Also one has

$$\begin{aligned} \xi^{\psi(a)} &\equiv \xi^{E_g(a)} \bmod s \\ &\equiv g^{\frac{q-1}{s}E_g(a)} \bmod s \\ &\equiv g^{E_g\left(a^{\frac{q-1}{s}}\right)} \bmod s \\ &\equiv a^{\frac{q-1}{s}} \bmod s. \end{aligned}$$

Theorem 3.1.1. *Let s, r be positive integers, with $s|q-1$. Let g be a primitive element, $\xi = g^{\frac{q-1}{s}}$ be a primitive s-th root of unity in $\mathbb{F}_q$. Let $f(x) \in \mathbb{F}_q[x]$. Then the polynomial $h(x) = x^r f(x^{\frac{q-1}{s}})$ is a PP of $\mathbb{F}_q$ if and only if the following conditions hold:*

(i) $(r, \frac{q-1}{s}) = 1$,

(ii) $f(\xi^i) \neq 0$ *for all* $0 \leq i < s$,

(iii) $\psi\left(\frac{f(\xi^{i_1})}{f(\xi^{i_2})}\right) \not\equiv r(i_2 - i_1) \bmod s$, *for all* $0 \leq i_1 < i_2 < s$.

Proof. Let $h(x)$ be a PP of $\mathbb{F}_q$. Then, $f(c^{\frac{q-1}{s}}) \neq 0$, for all $c \in \mathbb{F}_q^*$, since $h(0) = 0$. That is $f(x) \neq 0$, for any s-th root of unity x in $\mathbb{F}_q$. Since ξ is already an s-th root of unity in $\mathbb{F}_q$, we have

$$f(\xi^i) \neq 0 \text{ for all } 0 \leq i < s.$$

So (ii) is satisfied. For the rest of the proof, we will assume that (ii) holds and show that $h(x)$ is a PP if and only if (i) and (iii) are satisfied. From the definition of E_g, it follows that $h(x)$ is a PP of $\mathbb{F}_q$ if and only if $E_g(h(g^t)) \bmod q-1$ is the complete residue system modulo $(q-1)$, for $0 \leq t \leq q-2$.

Note that for all such t , we can write

$$t = sj + i, \text{ where } 0 \leq j < \frac{q-1}{s},\ 0 \leq i < s.$$

Therefore,

$$\begin{aligned} E_g(h(g^t)) &= E_g(h(g^{sj+i})) \\ &= E_g\left(g^{(sj+i)r} f\left(g^{(sj+i)\frac{q-1}{s}}\right)\right) \\ &= E_g(g^{(sj+i)r}) + E_g\left(f\left(g^{i\frac{q-1}{s}}\right)\right) \\ &= (sj+i)r + E_g(f(\xi^i)) \\ &= s(rj) + ri + E_g(f(\xi^i)). \end{aligned} \tag{3.2}$$

Now assume that (i) and (iii) are satisfied and let

$$E_g(h(g^{t_1})) = E_g(h(g^{t_2})),$$

for some $t_1 = j_1 s + i_1$ and $t_2 = j_2 s + i_2$ where $0 \leq j_1, j_2 < \frac{q-1}{s}$, $0 \leq i_1, i_2 < s$.

Then from (3.2),

$$s(rj_1) + ri_1 + E_g(f(\xi^{i^1})) \equiv s(rj_2) + ri_2 + E_g(f(\xi^{i^2})) \bmod (q-1),$$

equivalently,

$$\begin{aligned} sr(j_2 - j_1) + r(i_2 - i_1) - E_g\left(\frac{f(\xi^{i_1})}{f(\xi^{i_2})}\right) &\equiv 0 \bmod (q-1), \\ sr(j_2 - j_1) + r(i_2 - i_1) - \psi\left(\frac{f(\xi^{i_1})}{f(\xi^{i_2})}\right) &\equiv 0 \bmod (q-1). \end{aligned} \tag{3.3}$$

Note that if $i_1 \neq i_2$, (iii) implies

$$r(i_2 - i_1) - \psi\left(\frac{f(\xi^{i_1})}{f(\xi^{i_2})}\right) \not\equiv 0 \bmod s,$$

and since s is a divisor of $q-1$, (3.3) is not possible. Thus,

$$i_1 = i_2$$

so that

$$\begin{aligned} sr(j_2 - j_1) &\equiv 0 \mod (q-1), \\ r(j_2 - j_1) &\equiv 0 \mod (\frac{q-1}{s}). \end{aligned} \tag{3.4}$$

As $0 \leq j_1, j_2 < \frac{q-1}{s}$ and $(r, \frac{q-1}{s}) = 1$, (3.4) holds if and only if $j_1 = j_2$. Hence,

$$t_1 = j_1 s + i_1 = j_2 s + i_2 = t_2,$$

that is $h(x)$ is one-to-one.

Conversely assume that $h(x)$ is one-to-one. We will show that (i) and (iii) hold. First assume that (iii) does not hold. Then for $j_1 = j_2$ and for some distinct values of i_1 and i_2, with $0 \leq i_1, i_2 < s$ the equation in (3.3) holds contradicting to $h(x)$ being one-to-one. So (iii) necessarily holds. Now assume that (i) does not hold. Then in (3.3), we can take $i_1 = i_2$, so that $r(j_2 - j_1) \equiv 0 \bmod (\frac{q-1}{s})$. But since $(r, \frac{q-1}{s}) = 1$, we can find $0 \leq j_1 \neq j_2 < \frac{q-1}{s}$ satisfying the equation (3.3), which is a contradiction to h being one-to-one. Therefore (i) holds. □

Corollary 3.1.1. *Let $s, r \in N$, with $s|q-1$ and $(r, q-1) = 1$. Then the polynomial $f(x) = x^r(g(x^{\frac{q-1}{s}}))^s$ is a PP of $\mathbb{F}_q$ if and only if $g(x^{\frac{q-1}{s}})$ has no non-zero root in $\mathbb{F}_q$.*

Proof. Since $(r, q-1) = 1$, $(r, \frac{q-1}{s}) = 1$ so the condition (i) in Theorem 3.1.1 is satisfied. Suppose

$$p(x) = (g(x^{\frac{q-1}{s}}))^s,$$

Then, for $0 \leq i_1 < i_2 < s$,

$$\begin{aligned} \psi\left(\frac{p(\xi^{i_1})}{p(\xi^{i_2})}\right) &= \psi\left(\frac{g(\xi^{i_1})^s}{g(\xi^{i_2})^s}\right) \\ &= \psi\left(\left(\frac{g(\xi^{i_1})}{g(\xi^{i_2})}\right)^s\right) \\ &\equiv 0 \bmod s. \end{aligned} \tag{3.5}$$

Since $(r, s) = 1$ and $i_1 \not\equiv i_2 \bmod s$ from (3.5) it follows that

$$\psi\left(\frac{p(\xi^{i_1})}{p(\xi^{i_2})}\right) \not\equiv r(i_2 - i_1) \bmod s.$$

Hence the condition (iii) in Theorem 3.1.1 is also satisfied. Now it is clear that $f(x)$ is a PP of $\mathbb{F}_q$ if and only if the condition (ii) in Theorem 3.1.1 holds or equivalently $g(x^{\frac{q-1}{s}})$ has no non-zero root in $\mathbb{F}_q$. □

3.2 Binomial Permutation Poynomials

In this section we will investigate the permutation properties of the binomials $ax^i + bx^j + c$ over $\mathbb{F}_q$ following [3] and [13]. We will consider the binomial $x^i - \alpha x^j$ instead of $ax^i + bx^j + c$, where $\alpha = -a^{-1}b \in \mathbb{F}_q$, since their permutation properties are the same by Lemma 1.3.2.

Theorem 3.2.1. *Let $f(x) = x^i - \alpha x^j, 1 \leq j < i, \alpha \in \mathbb{F}_q^*$. Let $(i, j) = d$, and $i = i'd, j = j'd$, so that $(i', j') = 1$. Then, $f(x)$ is a PP of $\mathbb{F}_q$ if and only if $g(x) = x^{i'} - \alpha x^{j'}$ is a PP of $\mathbb{F}_q$ and $(d, q-1) = 1$.*

Proof. We can write $f(x) = (x^d)^{i'} - \alpha(x^d)^{j'}$. Thus, $f(x) = g(x^d)$, where $g(x) = x^{i'} - \alpha x^{j'}$. Now from Lemma 1.3.1, $f(x)$ is a PP of $\mathbb{F}_q$ if and only if $g(x)$ and x^d are PPs of $\mathbb{F}_q$. But x^d is a PP of $\mathbb{F}_q$ if and only if $(d, q-1) = 1$. So the result follows. □

In what follows $\mathbb{F}_q^{[i]}$ denotes the elements of $\mathbb{F}_q$ which are *i-th* powers, i.e. $\alpha \in \mathbb{F}_q^{[i]}$ if and only if there exists an element $\gamma \in \mathbb{F}_q$ such that $\alpha = \gamma^i$.

Theorem 3.2.2. *Let $f(x) = x^i - \alpha x^j, 1 \leq j < i, \alpha \in \mathbb{F}_q^*$. If $\alpha \in \mathbb{F}_q^{[i-j]}$, then $f(x)$ is not a PP of $\mathbb{F}_q$.*

Proof. Since $\alpha \neq 0$ and 0 is already a root of $f(x) = x^j(x^{i-j} - \alpha)$, if $\alpha \in \mathbb{F}_q^{[i-j]}$, $f(x)$ will have more than than one root, which implies that it is not a PP of $\mathbb{F}_q$. □

Lemma 3.2.1. *Let $\alpha \in \mathbb{F}_q$ and $0 \leq i \leq q-2$. Then $\alpha \notin \mathbb{F}_q^{[i]}$ if and only if $\alpha^{\frac{q-1}{d}} \neq 1$, where $d = (i, q-1)$.*

Proof. Since $d = (i, q-1)$, we can write,

$$d = ai + b(q-1) \text{ for some } a, b \in Z.$$

Assume that $\alpha \notin \mathbb{F}_q^{[i]}$ and $\alpha^{\frac{q-1}{d}} = 1$. Let β be a primitive element of $\mathbb{F}_q$ and $\alpha = \beta^k$ for some $0 \leq k < q-1$. Then

$$\begin{aligned} (\beta^k)^{\frac{q-1}{d}} &= 1, \\ q-1 \;\; &| \;\; k\frac{q-1}{d}, \\ d \;\; &| \;\; k. \end{aligned}$$

Let $k = dt$ for some $0 \leq t < \frac{q-1}{d}$. Then,

$$\begin{aligned} \alpha &= \beta^{dt} \\ &= (\beta^t)^{ai+b(q-1)} \\ &= (\beta^{q-1})^{bt} + (\beta^{ta})^i \\ &= (\beta^{ta})^i \end{aligned}$$

which contradicts to $\alpha \notin \mathbb{F}_q^{[i]}$. For the converse assume that $\alpha \in \mathbb{F}_q^{[i]}$. We want to show that $\alpha^{\frac{q-1}{d}} = 1$. Since $\alpha \in \mathbb{F}_q^{[i]}$, $\alpha = \gamma^i$ for some $\gamma \in \mathbb{F}_q$, $1 \leq i \leq q-1$. Now if $i = di'$,

$$\begin{aligned} \alpha^{\frac{q-1}{d}} &= \gamma^{i\frac{q-1}{d}} \\ &= \gamma^{di'\frac{q-1}{d}} \\ &= (\gamma^{q-1})^{i'} \\ &= 1. \end{aligned}$$

□

Corollary 3.2.1. *Let $f(x) = x^i - \alpha x^j \in \mathbb{F}_q[x], 1 \leq j < i, \alpha \neq 0$. Also let $d = (i-j, q-1)$. Then $f(x)$ is not a PP of $\mathbb{F}_q$ in any of the following cases:*

(i) $i = j + 1$,

(ii) $\alpha = 1$,

(iii) $\alpha = -1$ *and* $i - j$ *or* d *is odd,*

(iv) $d = 1$,

(v) $i - j$ *is a power of the characteristic of* $\mathbb{F}_q$.

Proof. **(i)** If $i - j = 1$, for any $\alpha \in \mathbb{F}_q^*, \alpha \in \mathbb{F}_q^{[i-j]} = \mathbb{F}_q$, therefore, from Theorem 3.2.2, $f(x)$ is not a PP of $\mathbb{F}_q$.

(ii) If $\alpha = 1$, since $1 = 1^{i-j}$, $\alpha \in \mathbb{F}_q^{[i-j]}$ for any $1 \leq j < i$, therefore, from Theorem 3.2.2, $f(x)$ is not a PP of $\mathbb{F}_q$.

(iii) If $\alpha = -1$ and $i - j$ is odd, then $-1 = (-1)^{i-j}$, that is $\alpha \in \mathbb{F}_q^{[i-j]}$. From Theorem 3.2.2, $f(x)$ is not PP of $\mathbb{F}_q$. Now let $i - j$ be even. If $\alpha = -1$ and d is odd, since $d = (i-j, q-1)$, $q-1$ must be odd, that is q is even. But in this case $-1 = 1$, and the claim follows by the argument in (ii).

(iv) If $d = 1$, $\alpha^{\frac{q-1}{d}} = \alpha^{q-1} = 1$ for all $\alpha \in \mathbb{F}_q^*$. So from Lemma 3.2.1, $\alpha \in \mathbb{F}_q^{[i-j]}$, and from Theorem 3.2.2, $f(x)$ is not a PP of $\mathbb{F}_q$.

(v) If $i - j$ is a power of the characteristic p of $\mathbb{F}_q$, that is $i - j = p^k$ for some $k \in N$, then $d = (i - j, q - 1) = (p^k, p^n - 1) = 1$, hence the rest follows from (iv).

□

The next Theorem is from [3] where Janphaisaeng et al present a new class of PPs.

Theorem 3.2.3. *Let $f(x) = x^i - \alpha x^j \in \mathbb{F}_q[x]$, $1 \leq j < i$. Assume that $i - j = q - 1, \alpha \neq 1$, and $(j, q - 1) = 1$. Then $f(x) \bmod (x^q - x)$ is a PP of $\mathbb{F}_q$.*

Proof. Write $f(x) = x^i - \alpha x^j = x^j(x^{i-j} - \alpha)$. In Corollary 3.1.1 setting

$$r = j,\ g(x) = x - \alpha,\ s = q - 1,$$

we obtain that $f(x) = x^r(g(x^s))^{\frac{q-1}{s}}$ is a PP of $\mathbb{F}_q$ if and only if $g(x^s) = x^{q-1} - \alpha$ has no nonzero root in $\mathbb{F}_q$. But since $\alpha \neq 1$ the polynomial $g(x^s)$ has no root in $\mathbb{F}_q$, implying that $f(x)$ is a PP of $\mathbb{F}_q$. □

The following Theorem states a criterion for binomial PPs, see [13].

Theorem 3.2.4. *Let $f(x) = x^i - \alpha x^j \in \mathbb{F}_q[x]$, $1 \leq j < i < q - 1$, $\alpha \neq 0$. Let $n = i - j$. If $f(x)$ is a PP of $\mathbb{F}_q$, then we have two cases:*

(i) *$i \not| q - 1 + n$*

(ii) *$i | q - 1 + n$ and if $ik = q - 1 + n$, then k is a multiple of the characteristic p of $\mathbb{F}_q$.*

Proof. Let $f(x) = x^i - \alpha x^j$ be a PP of $\mathbb{F}_q$ and assume that $i | q - 1 + n$. Then $ik = q - 1 + n$ for some $1 < k < q - 1$. Knowing that $f(x)$ is a PP of $\mathbb{F}_q$, and using the fact that

$$\sum_{c \in \mathbb{F}_q} c^t = \begin{cases} 0 & \text{if } 0 \leq t \leq q - 2 \\ -1 & \text{if } t = q - 1 \end{cases} \tag{3.6}$$

we get

$$\sum_{c \in \mathbb{F}_q} (c^i - \alpha c^j)^k \ = \ \sum_{c \in \mathbb{F}_q} c^k = 0. \tag{3.7}$$

On the other hand,

$$\sum_{c \in \mathbb{F}_q} (c^i - \alpha c^j)^k \ = \ \sum_{t=0}^{k} \binom{k}{t} (-\alpha)^t \sum_{c \in \mathbb{F}_q} c^{i(k-t)+jt}. \tag{3.8}$$

Combining (3.7) and (3.8), we obtain

$$\sum_{t=0}^{k} \binom{k}{t} (-\alpha)^t \sum_{c \in \mathbb{F}_q} c^{i(k-t)+jt} = 0. \tag{3.9}$$

But the only nonzero term in the sum (3.9) comes from $t = 1$ and it is

$$\begin{aligned} \binom{k}{1}(-\alpha) \sum_{c \in \mathbb{F}_q} c^{ik-i+j} &= k(-\alpha) \sum_{c \in \mathbb{F}_q} c^{(q-1+n)-n} \\ &= -k\alpha \sum_{c \in \mathbb{F}_q} c^{q-1} \\ &= k\alpha \end{aligned}$$

Therefore, $k\alpha = 0$ for $\alpha \in \mathbb{F}_q^*$, which shows that k is a multiple of p. □

Example 3.2.1. Let $f(x) = x^{35} + \alpha x^{19} \in \mathbb{F}_{125}$.

$$n = i - j = 16.$$

Since $35 | 124 + 16 = 140$, but $\frac{140}{35} = 4$ which is not a multiple of the characteristic 5, from Theorem 3.2.4, we conclude that $f(x)$ is not a PP of $\mathbb{F}_q$.

Theorem 3.2.5. *Let $f(x) = x^{p^i} - \alpha x^{p^j} \in \mathbb{F}_q[x]$ with $0 \leq j < i, \alpha \neq 0$. Then $f(x)$ is a PP of $\mathbb{F}_q$ if and only if $\alpha \notin \mathbb{F}_q^{[k]}$ where $k = p^i - p^j$.*

Proof. Let $f(x)$ be a PP of $\mathbb{F}_q$. Then from Theorem 3.2.2, it follows that $\alpha \notin \mathbb{F}_q^{[k]}$ where $k = p^i - p^j$. For the converse assume that $f(x)$ is not a PP of $\mathbb{F}_q$. We want to show that $\alpha \in \mathbb{F}_q^{[k]}$. Since $f(x)$ is not a PP of $\mathbb{F}_q$, there exist c_1, c_2 in $\mathbb{F}_q$, with $c_1 \neq c_2$, such that $f(c_1) = f(c_2)$. So,

$$\begin{aligned} c_1^{p^i} - \alpha c_1^{p^j} &= c_2^{p^i} - \alpha c_2^{p^j} \\ \alpha c_1^{p^j} - \alpha c_2^{p^j} &= c_1^{p^i} - c_2^{p^i} \\ \alpha (c_1 - c_2)^{p^j} &= (c_1 - c_2)^{p^i} \\ \alpha &= (c_1 - c_2)^{p^i - p^j}. \end{aligned}$$

Therefore $\alpha \in \mathbb{F}_q^{[k]}$ where $k = p^i - p^j$. □

3.3 Permutation Polynomials of the form $x^u(x^v + 1)$

Using Hermite's criterion, Wang gave the following characterization for a class of PPs of the form $x^u(x^v + 1)$ (see [15]).

Theorem 3.3.1. *let* $3|q-1$ *and*

$$f(x) = x^u(x^v+1) \in \mathbb{F}_q[x],$$

$u, v \in Z^+$, $(v, q-1) = \frac{q-1}{3}$. *Then* $f(x)$ *is a PP of* $\mathbb{F}_q$ *if and only if*

$$\left(u, \frac{q-1}{3}\right) = 1, u \not\equiv v \bmod 3 \text{ and } 2^{\frac{q-1}{3}} = 1 \text{ in } \mathbb{F}_q.$$

To prove this theorem we first need some lemmas.

Lemma 3.3.1. *If* $f(x) = x^u(x^v+1)$ *is a permutation polynomial in* $\mathbb{F}_q[x]$, *then*

$$(u, v, q-1) = 1.$$

Proof. Let $(u, v, q-1) = d$. We can write $f(x) = g(x^d)$ where $g(x) = x^{\frac{u}{d}}(x^{\frac{v}{d}} + a)$. Now let $x_1^d = x_2^d$ for some $x_1, x_2 \in \mathbb{F}_q$. Then, $g(x_1^d) = g(x_2^d)$, so that $f(x_1) = f(x_2)$. Since f is a permutation polynomial , it follows that $x_1 = x_2$, hence $h(x) = x^d$ is a permutation polynomial over $\mathbb{F}_q$. In this case, from the properties of binomial PPs, we have $(d, q-1) = 1$. But since we also know that $d|q-1$, $d = 1$. □

Lemma 3.3.2. *If* d *is odd,* $d|q-1$, $2^{\frac{q-1}{d}} \equiv 1 \bmod p$, *and* $(v, q-1) = \frac{q-1}{d}$, *then* $f(x) = x^u(x^v+1) = 0$ *has only one root, namely 0.*

Proof. Since $2^{\frac{q-1}{d}} \equiv 1 \bmod p$, p must be odd. If $f(x)$ has another root c in $\mathbb{F}_q$, then $f(c) = c^u(c^v+1) = 0$. But $c \neq 0$, so $c^v + 1 = 0$. Since $(v, q-1) = \frac{q-1}{d}$, $\exists r \in Z$ such that $\frac{q-1}{d}r = v$, so $(q-1)r = dv$, $(q-1)|vd$. And since $c^{q-1} = 1$ we have $c^{vd} = 1$.
But on the other hand, $c^{vd} = (c^v)^d = (-1)^d = -1$, as d is odd. This a contradiction since the characteristic p of $\mathbb{F}_q$ is odd, so that $-1 \neq 1$. Therefore there is no such c in $\mathbb{F}_q$. □

Lemma 3.3.3. *Let* $(v, q-1) = d, (u, d) = 1$ *and* $d \nmid t$. *Then,* $(x^u(x^v+1))^t \bmod (x^q - x)$ *has degree* $< q-1$.

Proof.

$$\begin{aligned}(x^u(x^v+1))^t &= x^{ut}(x^v+a)^t \\ &= x^{ut}\left(\sum_{i=1}^{t}\binom{t}{i}(x^v)^{t-i}a^i\right).\end{aligned}$$

Note that the reduction $f(x) \bmod (x^q - x)$ has a term with exponent $q-1$ if and only if $f(x)$ has a term with the exponent which is a multiple of $q-1$. Now if n is the degree of any term in the expansion, then

$$n = ut + vi \text{ for some } i = 1, \ldots, t.$$

Since $d|v$, we have $n \equiv ut \bmod d$. Also, since $(u,d)=1$ and $d \not| t$, we obtain that $d \not| n$ and therefore $q-1 \not| n$. $\square$

Now let $n,k \in \mathbb{Z}^+$, $b \in \mathbb{Z}$. Define the function

$$M(n,k,b) = \sum_{i=1}^{\lfloor \frac{n-c}{k} \rfloor} \binom{n}{ki+c},$$

where $b \equiv c \bmod k$. Then clearly, if $a \equiv b \bmod k$, then $M(n,k,a) = M(n,k,b)$. And if $b \equiv c \bmod k$, using the identity

$$\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1}$$

we obtain

$$\begin{aligned} M(n+1,k,b) &= \sum_{i=0}^{\lfloor \frac{n+1-c}{k} \rfloor} \binom{n+1}{ki+c} \\ &= \sum_{i=0}^{\lfloor \frac{n+1-c}{k} \rfloor} \binom{n}{ki+c} + \sum_{i=0}^{\lfloor \frac{n+1-c}{k} \rfloor} \binom{n}{ki+c-1} \\ &= \sum_{i=0}^{\lfloor \frac{n-c}{k} \rfloor} \binom{n}{ki+c} + \sum_{i=0}^{\lfloor \frac{n+1-c}{k} \rfloor} \binom{n}{ki+c-1} \\ &= M(n,k,b) + M(n,k,b-1). \end{aligned} \tag{3.10}$$

Lemma 3.3.4. *If $2n+c \equiv 0 \bmod 3$, then $M(2n,3,c) = \frac{2^{2n}+2}{3}$. If $2n+c \not\equiv 0 \bmod 3$, then $M(2n,3,c) = \frac{2^{2n}-1}{3}$.*

Proof. To prove the Lemma, we will divide the even numbers into three parts, namely, $6n, 6n+2, 6n+4$, according to their remainders modulo 3, and consider the cases seperately. First note that

$$\begin{aligned} M(6n,3,0) &= \sum_{i=0}^{\lfloor \frac{6n}{3} \rfloor} \binom{6n}{3i} \\ &= \binom{6n}{0} + \binom{6n}{3} + \ldots + \binom{6n}{6n} \\ &= 1 + \frac{2^{6n}-1}{3} \\ &= \frac{2^{6n}+2}{3}, \end{aligned}$$

$$\begin{aligned} M(6n,3,1) &= \sum_{i=0}^{\lfloor \frac{6n-1}{3} \rfloor} \binom{6n}{3i+1} \\ &= \binom{6n}{1} + \binom{6n}{4} + \ldots + \binom{6n}{6n-2} \\ &= \frac{2^{6n}-1}{3}, \end{aligned}$$

$$\begin{aligned} M(6n,3,2) &= \sum_{i=0}^{\lfloor \frac{6n-2}{3} \rfloor} \binom{6n}{3i+2} \\ &= \binom{6n}{2} + \binom{6n}{5} + \ldots + \binom{6n}{6n-1} \\ &= \frac{2^{6n}-1}{3}, \end{aligned}$$

so that

$$\begin{aligned} M(6n+1,3,0) &= M(6n,3,0) + M(6n,3,2) = \frac{2^{6n+1}+1}{3} \\ M(6n+1,3,1) &= M(6n,3,0) + M(6n,3,1) = \frac{2^{6n+1}+1}{3} \\ M(6n+1,3,2) &= M(6n,3,1) + M(6n,3,2) = \frac{2^{6n+1}-2}{3} \\ M(6n+2,3,0) &= M(6n+1,3,0) + M(6n+1,3,2) = \frac{2^{6n+2}-1}{3} \\ M(6n+2,3,1) &= M(6n+1,3,0) + M(6n+1,3,1) = \frac{2^{6n+2}+2}{3} \\ M(6n+2,3,2) &= M(6n+1,3,1) + M(6n+1,3,2) = \frac{2^{6n+2}-1}{3} \\ M(6n+3,3,0) &= M(6n+2,3,0) + M(6n+2,3,2) = \frac{2^{6n+3}-2}{3} \\ M(6n+3,3,1) &= M(6n+2,3,0) + M(6n+2,3,1) = \frac{2^{6n+3}+1}{3} \\ M(6n+3,3,2) &= M(6n+2,3,1) + M(6n+2,3,2) = \frac{2^{6n+3}+1}{3} \\ M(6n+4,3,0) &= M(6n+3,3,0) + M(6n+3,3,2) = \frac{2^{6n+4}-1}{3} \\ M(6n+4,3,1) &= M(6n+3,3,0) + M(6n+3,3,1) = \frac{2^{6n+4}-1}{3} \\ M(6n+4,3,2) &= M(6n+3,3,1) + M(6n+3,3,2) = \frac{2^{6n+4}+2}{3} \\ M(6n+5,3,0) &= M(6n+4,3,0) + M(6n+4,3,2) = \frac{2^{6n+5}+1}{3} \\ M(6n+5,3,1) &= M(6n+4,3,0) + M(6n+4,3,1) = \frac{2^{6n+5}-2}{3} \\ M(6n+5,3,2) &= M(6n+5,3,1) + M(6n+5,3,2) = \frac{2^{6n+5}+1}{3}. \end{aligned}$$

□

Now we are ready to prove the Theorem 3.3.1

Proof. First suppose that $f(x)$ is a PP. Since $(v, q-1) = \frac{q-1}{3}$, v can be expressed as $v = v_1 \frac{q-1}{3}$ for some $v_1 \in Z$. Here,

$$3 \not| v_1,$$

since, otherwise if $3|v_1$ then $v_1 = 3k$, $k \in Z$, and $v = 3k\frac{q-1}{3} = k(q-1)$, so that $(v, q-1) = (k(q-1), q-1) = q-1$, a contradiction. Also since $3 \not| v_1$, $v_1 \equiv 1 \bmod 3$

or $v_1 \equiv 2 \bmod 3$. If $v_1 \equiv 1 \bmod 3$, then $v_1 - 1 \equiv 0 \bmod 3$, and if $v_1 \equiv 2 \bmod 3$, then $v_1 + 1 \equiv 0 \pmod 3$. Therefore,

$$v_1^2 \equiv 1 \bmod 3.$$

Consider

$$\begin{aligned}(f(x))^{\frac{q-1}{3}} &= (x^u(x^v+1))^{\frac{q-1}{3}} \\ &= x^{u\frac{q-1}{3}} \sum_{i=1}^{\frac{q-1}{3}} \binom{\frac{q-1}{3}}{i} x^{vi}. \end{aligned} \tag{3.11}$$

Now we prove that the coefficient of x^{q-1} in the reduction $(f(x))^{\frac{q-1}{3}} \bmod (x^q - x)$ is $M\left(\frac{q-1}{3}, 3, -v_1 u\right)$. If n is the degree of any term in the expansion of $(f(x))^{\frac{q-1}{3}}$, from (3.11) $n = u\frac{q-1}{3} + vi$, for some $i = 0, \ldots, \frac{q-1}{3}$. Now for $i = -v_1 u$,

$$\begin{aligned} u\frac{q-1}{3} + vi &= u\frac{q-1}{3} + v(-v_1 u) \\ &= u\frac{q-1}{3} + v_1\frac{q-1}{3}(-v_1 u) \\ &= \frac{q-1}{3}u(1 - v_1^2). \end{aligned}$$

But, since $v_1^2 \equiv 1 \bmod 3$, $3|u(1-v_1^2)$ so that $q-1|\frac{q-1}{3}u(1-v_1^2)$. Thus, for $i = -v_1 u$, $(q-1)|u\frac{q-1}{3} + vi$. Also note that, if $(q-1)|u\frac{q-1}{3} + vi$ for some $i = 0, \ldots, q-1$, then $(q-1)|u\frac{q-1}{3} + v(i+3)$, since in this case

$$\begin{aligned} u\frac{q-1}{3} + v(i+3) &= \left(u\frac{q-1}{3} + vi\right) + 3v \\ &= \left(u\frac{q-1}{3} + vi\right) + v_1(q-1). \end{aligned}$$

So we conclude that, the coefficient of x^{q-1} in $(f(x))^{\frac{q-1}{3}} \bmod (x^q - x)$ is

$$M(\frac{q-1}{3}, 3, -v_1 u) = \sum_{i=0}^{\left\lfloor \frac{\frac{q-1}{3} - c}{3} \right\rfloor} \binom{\frac{q-1}{3}}{3i + c} \tag{3.12}$$

where $c \equiv -v_1 u \bmod 3$.

Similarly, the coefficient of x^{q-1} in the reduction $(f(x))^{\frac{2(q-1)}{3}} \bmod (x^q - x)$ is

$$M(\frac{2(q-1)}{3}, 3, -2v_1 u). \tag{3.13}$$

Since we assumed that $f(x) = x^u(x^v+1)$ is a PP from Lemma 3.3.1,

$$(u, v, q-1) = (u, \frac{q-1}{3}) = 1.$$

Assuming that $f(x)$ is a PP, by Hermite's criterion for $t = \frac{q-1}{3}$, $(f(x))^t \bmod (x^q - x)$ has degree $< q-1$. Therefore

$$M(\frac{q-1}{3}, 3, -v_1 u) = 0.$$

But from Lemma 3.3.4,

$$M(\frac{q-1}{3}, 3, -v_1u) \ = \frac{2^{\frac{q-1}{3}}-1}{3} \quad \text{or} \quad \frac{2^{\frac{q-1}{3}}+2}{3}$$

Since $(2^{\frac{q-1}{3}})^3 = 2^{q-1} = 1$ in $\mathbb{F}_q$, and $q \equiv 1 \bmod 3$, $2^{\frac{q-1}{3}} \neq -2$. Hence, from Lemma 3.3.4,

$$M(\frac{q-1}{3}, 3, -v_1u) = \frac{2^{\frac{q-1}{3}}-1}{3} = 0$$

so that $2^{\frac{q-1}{3}} = 1$ and $\frac{q-1}{3} - v_1u \not\equiv 0 \bmod 3$. Using $3 \not| v_1$,

$$v_1(\frac{q-1}{3} - v_1u) = v - v_1^2u \not\equiv 0 \bmod 3$$

and since $v_1^2 \equiv 1 \bmod 3$, $v \not\equiv u \bmod 3$.

Conversely, let

$$(u, \frac{q-1}{3}) = 1 \ , \ u \not\equiv v \bmod 3 \ \text{ and } \ 2^{\frac{q-1}{3}} = 1.$$

In Lemma 3.3.4, let $d = 3$, as we know that $3|q-1$, we have $2^{\frac{q-1}{3}} \equiv 1 \bmod 3$, and $(v, q-1) = \frac{q-1}{3}$. Then, finding such an odd number, we conclude that the only root of $f(x) = x^u(x^v+1)$ is 0. Since $(v, q-1) = \frac{q-1}{3}$, we have $(u, \frac{q-1}{3}) = 1$. Now in Lemma 3.3.3, let $d = \frac{q-1}{3}$. Then, for all t such that $\frac{q-1}{3} \not| t$,

$$(f(x))^t \bmod (x^q - x) \text{ has degree } < q-1.$$

Now for $t = \frac{q-1}{3}$, we know that the coefficient of x^{q-1} in $(f(x))^{\frac{(q-1)}{3}} \bmod (x^q - x)$ is $M(\frac{q-1}{3}, 3, -v_1u)$ and since $v \not\equiv u \bmod 3$, we have $\frac{q-1}{3} - v_1u \not\equiv 0 \bmod 3$. Then according to Lemma 3.3.4

$$M(\frac{q-1}{3}, 3, -v_1u) = \frac{2^{\frac{q-1}{3}}-1}{3} = 0,$$

where we used the assumption that $2^{\frac{q-1}{3}} = 1$ in the second identity. Similarly, since $\frac{2(q-1)}{3} - 2v_1u \not\equiv 0 \bmod 3$, the coefficient of x^{q-1} in $(f(x))^{\frac{2(q-1)}{3}} \bmod (x^q - x)$ is $M(\frac{2(q-1)}{3}, 3, -2v_1u)$ and from Lemma 3.3.4, it follows that

$$M(\frac{2(q-1)}{3}, 3, -2v_1u) = \frac{2^{\frac{2(q-1)}{3}}-1}{3} = 0.$$

Therefore, $f(x)^t \bmod (x^q - x)$ has degree $< q-1$ for $t = \frac{q-1}{3}$ and $\frac{2(q-1)}{3}$. Finally, by Hermite's criterion, we conclude that $f(x)$ is a PP. □

Example 3.3.1. In this example using Theorem 3.3.1, we will write all PPs of the form $x^u(x^v+1)$ in $\mathbb{F}_{127}$ satisfying $(v, 126) = 1$. First note that

$$2^{\frac{127-1}{3}} = 2^{42} = 1 \ in \ \mathbb{F}_{127}.$$

Also the assumption of the Theorem requires that $(v, 126) = 42$. So there exist two values for v, namely, 42, 84. Hence, keeping in mind that $deg(f(x)) \leq 125$, we have two cases:

Case 1 Let $v = 42$. Then $f(x) = x^u(x^{42} + 1)$ is a PP of $\mathbb{F}_{127}$ if and only if $(u, 42) = 14$ (in which case $u \not\equiv 0 \bmod 3$ is necessarily satisfied). Thus, all the possible values for u corresponding to $v = 42$ are

$$1, 4, 5, 11, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 51, 53, 55, 57, 59, 61, 65, 67, 71, 73, 79, 83.$$

Case 2 Let $v = 84$. Then $f(x) = x^u(x^{84} + 1)$ is a PP of $\mathbb{F}_{127}$ if and only if $(u, 84) = 1$ (in which case $u \not\equiv 0 \bmod 3$ is necessarily satisfied). Thus, all the possible values for u corresponding to $v = 84$ are

$$1, 4, 5, 11, 17, 19, 23, 25, 29, 31, 35, 37, 41.$$

Therefore, all PPs of the form $x^u(x^v + 1)$ in $\mathbb{F}_{127}$ are:

$$\begin{gathered}
x(x^{42}+1),\ x^4(x^{42}+1),\ x^5(x^{42}+1),\ x^{11}(x^{42}+1),\ x^{17}(x^{42}+1) \\
x^{19}(x^{42}+1),\ x^{23}(x^{42}+1),\ x^{25}(x^{42}+1),\ x^{29}(x^{42}+1),\ x^{31}(x^{42}+1) \\
x^{35}(x^{42}+1),\ x^{37}(x^{42}+1),\ x^{41}(x^{42}+1),\ x^{43}(x^{42}+1),\ x^{47}(x^{42}+1) \\
x^{51}(x^{42}+1),\ x^{53}(x^{42}+1),\ x^{55}(x^{42}+1),\ x^{57}(x^{42}+1),\ x^{59}(x^{42}+1) \\
x^{61}(x^{42}+1),\ x^{65}(x^{42}+1),\ x^{67}(x^{42}+1),\ x^{71}(x^{42}+1),\ x^{73}(x^{42}+1) \\
x^{79}(x^{42}+1),\ x^{83}(x^{42}+1),\ x(x^{84}+1),\ x^4(x^{84}+1),\ x^5(x^{84}+1) \\
x^{11}(x^{84}+1),\ x^{17}(x^{84}+1),\ x^{19}(x^{84}+1),\ x^{23}(x^{84}+1),\ x^{25}(x^{84}+1) \\
x^{29}(x^{84}+1),\ x^{31}(x^{84}+1),\ x^{35}(x^{84}+1),\ x^{37}(x^{84}+1),\ x^{41}(x^{84}+1).
\end{gathered} \tag{3.14}$$

3.4 Permutation Poynomials of the form $x^{\frac{q+1}{2}} + ax$

Before giving a criterion related to polynomials of the form $x^{\frac{q+1}{2}} + ax$ we will first recall that the quadratic character η of a finite field $\mathbb{F}_q$ of odd characteristic is defined by

$$\eta(c) = \begin{cases} 1 & \text{if } c \text{ is square in } \mathbb{F}_q^* \\ -1 & \text{otherwise} \end{cases} \tag{3.15}$$

Note that as a convention we let $\eta(0) = 0$.

Lemma 3.4.1. *Let c be a nozero element in $\mathbb{F}_q$. Then,*

$$c^{\frac{q-1}{2}} = \begin{cases} 1 & \text{if } \eta(c) = 1 \\ -1 & \text{if } \eta(c) = -1 \end{cases} \tag{3.16}$$

Theorem 3.4.1. *Let q be a odd prime power and $f(x) = x^{\frac{q+1}{2}} + ax \in \mathbb{F}_q[x]$. Then $f(x)$ is a PP of $\mathbb{F}_q$ if and only if $\eta(a^2 - 1) = 1$.*

Proof. We will show that $f(x) = x^{\frac{q+1}{2}} + ax$ is not a PP if and only if $\eta(a^2 - 1) \neq 1$. First assume that $f(x) = x^{\frac{q+1}{2}} + ax$ is not a PP, therefore not one-to-one. Then we have two cases:

Case 1 There exists an element $c \in \mathbb{F}_q^*$ such that f(c)=f(0)=0. In this case,

$$\begin{aligned} c^{\frac{q+1}{2}} + ac &= 0 \\ a &= -c^{\frac{q-1}{2}} \end{aligned}$$

$$\eta(a^2 - 1) = \eta(c^{q-1} - 1) = \eta(0) = 0.$$

Case 2 There exist elements $b, c \in \mathbb{F}_q^*$ with $b \neq c$, such that $f(b) = f(c)$. Then

$$b^{\frac{q+1}{2}} + ab = c^{\frac{q+1}{2}} + ac \tag{3.17}$$

$$b(b^{\frac{q-1}{2}} + a) = c(c^{\frac{q-1}{2}} + a)$$

$$bc^{-1} = (c^{\frac{q-1}{2}} + a)(b^{\frac{q-1}{2}} + a)^{-1} \tag{3.18}$$

Now if $\eta(b) = \eta(c)$, from Lemma 3.4.1 it follows that

$$b^{\frac{q+1}{2}} = c^{\frac{q+1}{2}}. \tag{3.19}$$

Inserting (3.19) in (3.17), we obtain $b = c$, which is a contradiction with the choice of b and c. Therefore $\eta(b) \neq \eta(c)$.

Since $b, c \in \mathbb{F}_q^*$, without loss of generality, we can assume that $\eta(b) = 1$ and $\eta(c) = -1$. Then we have

$$b^{\frac{q-1}{2}} = 1 \text{ and } c^{\frac{q-1}{2}} = -1.$$

and (3.15) becomes

$$bc^{-1} = (a + 1)^{-1}(a - 1).$$

Hence,

$$\begin{aligned}\eta(a^2-1) &= \eta((a+1)(a-1)) \\ &= \eta((a+1)^{-1}(a-1)) \\ &= \eta(bc^{-1}) \\ &= \eta(b)\eta(c) \\ &= -1\end{aligned}$$

Therefore both in Case 1 and Case 2, we have $\eta(a^2-1) \neq 1$.

Now, conversely assume that $\eta(a^2-1) \neq 1$. We consider two cases:

Case 1 Let $\eta(a^2-1) = 0$. In this case $a^2-1=0$, hence $a=1$ or -1. In either case, there exists an element $c \in \mathbb{F}_q^*$ such that $\eta(c) = -a$, i.e. $c^{\frac{q-1}{2}} = -a$. But then

$$\begin{aligned}f(c) &= c^{\frac{q+1}{2}} + ca \\ &= c(c^{\frac{q-1}{2}} + a) \\ &= 0.\end{aligned}$$

Hence $f(x)$ is not one-to-one, thereby is not a PP of $\mathbb{F}_q$.

Case 2 Let $\eta(a^2-1) = -1$.

$$\begin{aligned}f((a+1)(a-1)^{-1}) &= (a+1)(a-1)^{-1}((a+1)^{\frac{q-1}{2}}(a-1)^{\frac{-q+1}{2}} + a) \\ &= \frac{a+1}{a-1}(a-1) \\ &= a+1 \\ &= f(1).\end{aligned}$$

And since $(a+1)(a-1)^{-1} \neq 1$, we conclude that $f(x)$ is not one-to-one, therefore it is not a PP of $\mathbb{F}_q$. □

Bibliography

[1] Chung, K.O. *Permutation Binomials over Finite Fields*, 2004.

[2] Das, P. *The Number of Permutation Polynomials of a Given Degree Over a Finite Field* , Finite Fields Appl. **8**, 478-490, 2002.

[3] Janphaisaeng, S. , Laohakosol, V. and Harnchoowong, A. *Some New Classes of Permutation Polynomials*, Science Asia, **28**, 401-405, 2002.

[4] Konyagin, S. and Pappalardi, F. *Enumerating Permutation Polynomials Over Finite Fields by Degree*, Finite Fields Appl. **8**, 548-553, 2002.

[5] Konyagin, S. and Pappalardi, F. *Enumerating Permutation Polynomials Over Finite Fields by Degree II*, Finite Fields Appl. **12**, 26-37, 2006.

[6] Lidl, R. and Mullen, G.L. *When Does a Polynomial over a Finite Field Permute the Elements of the Field* , The American Mathematical Montly, Vol.95, No.3, 243-246, 1998.

[7] Lidl, R. and Mullen, G.L. *When Does a Polynomial over a Finite Field Permute the Elements of the Field, II*, The American Mathematical Montly, Vol.100, No.1, 71-74, 1993.

[8] Lidl, R. and Niederreiter, H. *Introduction to Finite Fields and Their Applications*, Cambridge Univ. Press, Cambridge, 1994.

[9] Malnenuto, C. and Pappalardi, F. *Enumerating Permutation Polynomials I: Permuatations with Non-Maximal Degree*, Finite Fields Appl. **8**, 531-547, 2002.

[10] Mullen, G.L. *Permutation Polynomials over Finite Fields, Finite Fields, Coding Theory, and Advances in Communications and Computing*, Marcel Dekker, NY, 131-151, 1993.

[11] Niederreiter, H. and Robinson, K.H. *Complete Mappings of Finite Fields*, J. Austral. Math. Soc. **33**, 197-212, 1982.

[12] Shparlinski, I.E. *Finite Fields: Theory and Computation*, Kluver Academic Publishers, 1999.

[13] Small, C. *Permutation Binomials*, Internat. J. Math. and Math. Sci. **13**, 337-342, 1990 .

[14] Wan, D. and Lidl, R. *Permutation Polynomials of the Form* $x^r f(x^{\frac{q-1}{d}})$ *and their Group Structure*, Monaths. Math. **112**, 149-163, 1991.

[15] Wang, L. *On Permutation Polynomials*, Finite Fields Appl. **8**, 311-322, 2002.

[16] Wells, C. *The Degrees of Permutation Polynomials over Finite Fields*, Journal of Combinatorial Theory **7**, 49-55, 1969.