

พหุนามเรียงสับเปลี่ยนเหนือสนามจำกัด



นางสาวสุภาววรรณ จันทรีไพแสง

สถาบันวิทยบริการ

จุฬาลงกรณ์มหาวิทยาลัย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์

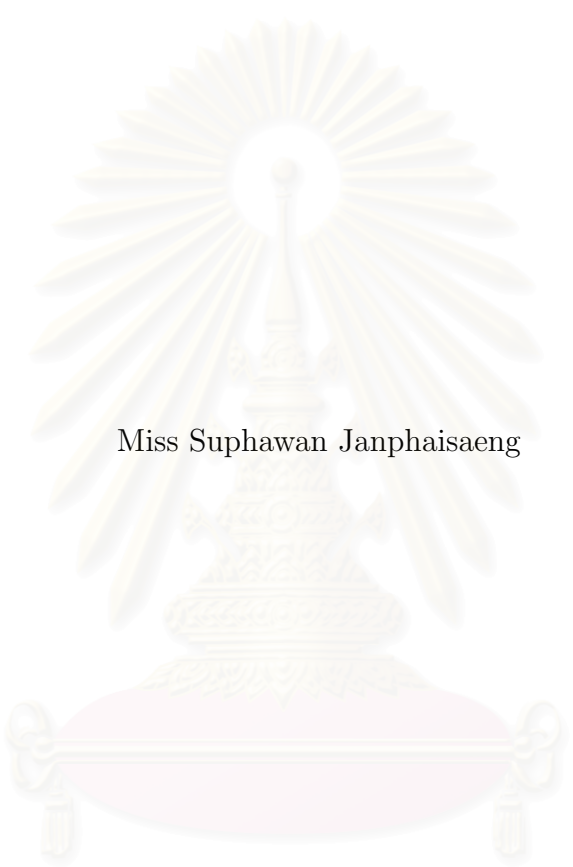
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2543

ISBN 974-130-927-9

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

PERMUTATION POLYNOMIALS OVER A FINITE FIELD



Miss Suphawan Janphaisaeng

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science in Mathematics

Department of Mathematics

Faculty of Science

Chulalongkorn University

Academic Year 2000

ISBN 974-130-927-9

Thesis Title : Permutation Polynomials over a Finite Field
By : Miss Suphawan Janphaisaeng
Field of Study : Mathematics
Thesis Advisor : Assistant Professor Ajchara Harnchoowong, Ph.D.
Thesis Co-advisor : Associate Professor Vichian Laohakosol, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial
Fulfillment of the Requirements for the Master 's Degree

..... Dean of Faculty of Science
(Associate Professor Wanchai Phothiphichitr, Ph.D.)

THESIS COMMITTEE

..... Chairman
(Associate Professor Chitchuab Paoin)

..... Thesis Advisor
(Assistant Professor Ajchara Harnchoowong, Ph.D.)

..... Thesis Co-advisor
(Associate Professor Vichian Laohakosol, Ph.D.)

..... Member
(Assistant Professor Utsanee Leerawat, Ph.D.)

สุภาวรรณ จันทร์ไพแสง : พหุนามเรียงสับเปลี่ยนเหนือสนามจำกัด (PERMUTATION POLYNOMIALS OVER A FINITE FIELD) อ. ที่ปรึกษา : ผศ.ดร. อัจฉรา หาญชูวงศ์, อ. ที่ปรึกษาร่วม : รศ.ดร. วิเชียร เลหา โกศล, 38 หน้า ISBN 974-130-927-9

วิทยานิพนธ์นี้มีสองส่วน ส่วนแรกเป็นการหาพหุนามเรียงสับเปลี่ยนแบบบรรทัดฐานระดับชั้น 6 ทั้งหมดเหนือสนามจำกัดที่มีอันดับ q เมื่อ q เป็นจำนวนเฉพาะสัมพัทธ์กับ 6 โดยใช้เกณฑ์ของเฮอรั่มิท-ดิกสัน (Hermite-Dickson) ส่วนที่สองเป็นการหาพหุนามเรียงสับเปลี่ยนประเภทใหม่ โดยส่วนใหญ่ขยายงานวิจัยที่มีมาก่อนของมอลลินและสมอล (Mollin and Small)



สถาบันวิทยบริการ จุฬาลงกรณ์มหาวิทยาลัย

ภาควิชา คณิตศาสตร์
สาขาวิชา คณิตศาสตร์
ปีการศึกษา 2543

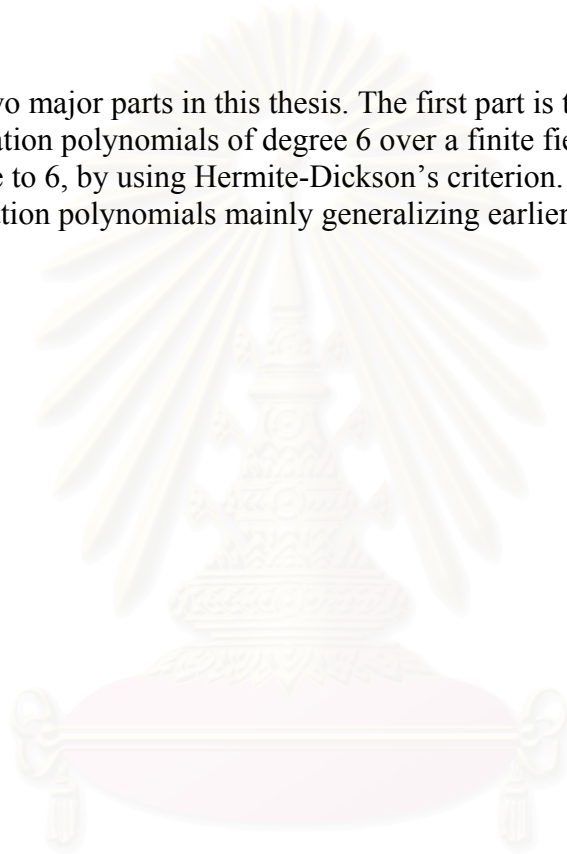
ลายมือชื่อนิสิต.....
ลายมือชื่ออาจารย์ที่ปรึกษา.....
ลายมือชื่ออาจารย์ที่ปรึกษาร่วม.....

4172507023 MAJOR : MATHEMATICS

KEYWORD : PERMUTATION POLYNOMIAL

SUPHAWAN JANPHAISAENG : PERMUTATION POLYNOMIALS
OVER A FINITE FIELD. THESIS ADVISOR : ASSISTANT PROFESSOR
AJCHARA HARNCHOOWONG, Ph.D. THESIS CO-ADVISOR :
ASSOCIATE PROFESSOR VICHIAN LAOHAKOSOL, Ph.D. 38pp.
ISBN 974-130-927-9

There are two major parts in this thesis. The first part is to determine all normalized permutation polynomials of degree 6 over a finite field of order q , where q is relatively prime to 6, by using Hermite-Dickson's criterion. The second part is to derive new permutation polynomials mainly generalizing earlier works of Mollin and Small.



สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Department **Mathematics**

Student's signature.....

Field of Study **Mathematics**

Advisor's signature.....

Academic year **2000**

Co-advisor's signature.....

ACKNOWLEDGEMENTS

I am greatly indebted to Associate Professor Dr.Vichian Laohakosol and Assistant Professor Dr.Ajchara Harnchoowong, my thesis co-advisor and my thesis advisor, for their untired offering me some thoughtful and helpful advice in preparing and writing this thesis. I would like to thank Associate Professor Chitchuab Paoin and Assistant Professor Dr.Utsanee Leerawat, my thesis committee, for their suggestions to this thesis. I would also like to thank all of the lecturers for their previous valuable lectures while studying.

In particular, I would like to express my gratitude to my family and my friends for their encouragement throughout my graduate study.



สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

CONTENTS

	Page
ABSTRACT IN THAI	iv
ABSTRACT IN ENGLISH	v
ACKNOWLEDGEMENTS	vi
CHAPTER	
I INTRODUCTION	1
II NORMALIZED PERMUTATION POLYNOMIALS OF DEGREE 6	8
III SOME NEW CLASSES OF PERMUTATION POLYNOMIALS	26
REFERENCES	37
VITA	38

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

CHAPTER I

INTRODUCTION

The general study of permutation polynomials started with Hermite who considered the case of finite prime fields. For the case of arbitrary finite fields, permutation polynomials were first systematically studied by Dickson. In order to understand permutation polynomials over a finite field, we collect here, mostly without proofs, basic properties of finite fields, basic definitions and theorems relating to permutation polynomials.

The proofs of these results can be found in [5], [6], [7] and [8].

A finite field is a field that contains only finitely many elements. The most familiar example is the field $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$, where p is a prime and the operations are addition and multiplication (mod p).

Theorem 1.1. *Let F be a finite field. Then*

- (1) *F has prime characteristic and*
- (2) *the multiplicative group F^* of all nonzero elements of F is cyclic.*
- (3) *the prime subfield of F is isomorphic to \mathbb{F}_p .*

Theorem 1.2. *Let F be a finite field. Then F has p^n elements where the prime p is the characteristic of F and n is the degree of F over its prime subfield.*

Lemma 1.3. *If F is a finite field with q elements, then every $a \in F$ satisfies $a^q = a$.*

Lemma 1.4. *If F is a finite field with q elements and K is a subfield of F , then the polynomial $x^q - x$ in $K[x]$ factors in $F[x]$ as*

$$x^q - x = \prod_{a \in F} (x - a)$$

and F is the splitting field of $x^q - x$ over K .

Theorem 1.5. For every prime p and every positive integer n there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over \mathbb{F}_p .

By Theorem 1.5, a field of order $q = p^n$ is unique up to isomorphism, it is denoted by \mathbb{F}_q and is called the **Galois field** of order q .

Next, we shall give basic definitions and theorems about permutation polynomials.

Definition 1.6. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be a **permutation polynomial** of \mathbb{F}_q if and only if it is a bijection map from \mathbb{F}_q to itself.

Example 1.7. Let $f(x) = x^5 + 2x^2 \in \mathbb{F}_7[x]$. Since $f(0) = 0, f(1) = 3, f(2) = 5, f(3) = 2, f(4) = 6, f(5) = 4$ and $f(6) = 1$ in \mathbb{F}_7 , f is a bijection map from \mathbb{F}_7 to \mathbb{F}_7 . Hence $f(x) = x^5 + 2x^2$ is a permutation polynomial of \mathbb{F}_7 .

Lemma 1.8. A polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial of \mathbb{F}_q if and only if one of the following conditions holds:

- (1) $f : c \mapsto f(c)$ is onto;
- (2) $f : c \mapsto f(c)$ is one-to-one;
- (3) $f(x) = a$ has a solution in \mathbb{F}_q for each $a \in \mathbb{F}_q$;
- (4) $f(x) = a$ has a unique solution in \mathbb{F}_q for each $a \in \mathbb{F}_q$.

Lemma 1.9. For $f, g \in \mathbb{F}_q[x]$ we have $f(c) = g(c)$ for all $c \in \mathbb{F}_q$ if and only if $f(x) \equiv g(x) \pmod{x^q - x}$.

Lemma 1.10. Let $a_0, a_1, a_2, \dots, a_{q-1}$ be elements of \mathbb{F}_q . Then the following two conditions are equivalent:

(1) $a_0, a_1, a_2, \dots, a_{q-1}$ are distinct;

$$(2) \sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \text{for } t = 0, 1, \dots, q-2, \\ -1 & \text{for } t = q-1. \end{cases}$$

The following criterion, proved first by Hermite for \mathbb{F}_p and later by Dickson for \mathbb{F}_q , is frequently used and provides an essential tool in discovering most permutation polynomials. Because of its importance, we give a complete proof.

Theorem 1.11. (*Hermite-Dickson's Criterion*) A polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial of \mathbb{F}_q if and only if the following two conditions hold:

(1) f has exactly one root in \mathbb{F}_q ;

(2) for each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \pmod{p}$, the reduction of $(f(x))^t \pmod{x^q - x}$ has degree $\leq q-2$.

Proof. Let f be a permutation polynomial of \mathbb{F}_q . Then (1) is trivial. Let t be any integer with $1 \leq t \leq q-2$ and $t \not\equiv 0 \pmod{p}$. Let $g(x) = \sum_{j=0}^{q-1} b_j^{(t)} x^j$ be the reduction of $(f(x))^t \pmod{x^q - x}$. By Lemma 1.9 and *Lagrange Interpolation Formula*, $g(x) = \sum_{c \in \mathbb{F}_q} (f(c))^t (1 - (x-c)^{q-1})$. Comparing the coefficient of x^{q-1} , we get $b_{q-1}^{(t)} = -\sum_{c \in \mathbb{F}_q} (f(c))^t$. According to Lemma 1.10, $b_{q-1}^{(t)} = 0$ for $t = 1, 2, \dots, q-2$, hence (2) holds.

Conversely, let (1) and (2) be satisfied. Then (1) implies $\sum_{c \in \mathbb{F}_q} (f(c))^{q-1} = 0 + \underbrace{1 + 1 + \dots + 1}_{q-1 \text{ times}} = -1$, while (2) implies $\sum_{c \in \mathbb{F}_q} (f(c))^t = 0$ for $1 \leq t \leq q-2$, $t \not\equiv 0 \pmod{p}$. From

$$\sum_{c \in \mathbb{F}_q} (f(c))^{tp^j} = \left(\sum_{c \in \mathbb{F}_q} (f(c))^t \right)^{p^j},$$

we get $\sum_{c \in \mathbb{F}_q} (f(c))^t = 0$ for $1 \leq t \leq q-2$, and $\sum_{c \in \mathbb{F}_q} (f(c))^t = \underbrace{1 + \dots + 1}_q = 0$ for $t = 0$. By Lemma 1.10, $f(c)$ are distinct for all $c \in \mathbb{F}_q$. Hence f is a permutation polynomial of \mathbb{F}_q . \square

Corollary 1.12. *If $d > 1$ is a divisor of $q - 1$, then there is no permutation polynomial of \mathbb{F}_q of degree d .*

Theorem 1.13. (1) *Every linear polynomial over \mathbb{F}_q is a permutation polynomial of \mathbb{F}_q .*

(2) *The monomial x^i is a permutation polynomial of \mathbb{F}_q if and only if $\text{g.c.d.}(i, q-1) = 1$.*

Proposition 1.14. *Let $f(x) \in \mathbb{F}_q[x]$, $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_q^*$. Then the following conditions are equivalent.*

- (1) f permutes \mathbb{F}_q ;
- (2) $f(x) + a$ permutes \mathbb{F}_q ;
- (3) $bf(x)$ permutes \mathbb{F}_q .

Definition 1.15. *A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be a **p -polynomial** over \mathbb{F}_q if and only if $f(x)$ is of the form $\sum_{i=0}^m a_i x^{p^i}$ where $m \in \mathbb{N}$.*

Example 1.16. $f(x) = x^8 + x^4 + x \in \mathbb{F}_4[x]$ is a 2-polynomial over \mathbb{F}_4 but $f(x) = x^8 + x^6 + x^4 + x \in \mathbb{F}_4[x]$ is not a 2-polynomial over \mathbb{F}_4 .

Theorem 1.17. *A p -polynomial*

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

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

Lemma 1.18. Let $f(x) = \sum_{i=1}^n c_i x^{m_i} \in \mathbb{F}_q[x]$ where $m_n > m_{n-1} > \dots > m_1 \geq 1$ and $\prod_{i=1}^n c_i \neq 0$. Suppose $e = \text{g.c.d.}(m_1, m_2, \dots, m_n)$. Then $f(x)$ is a permutation polynomial of \mathbb{F}_q if and only if $\text{g.c.d.}(e, q-1) = 1$ and $\sum_{i=1}^n c_i x^{m_i/e}$ is a permutation polynomial of \mathbb{F}_q .

Proposition 1.19. Let $f(x) = ax^i + bx^j + c \in \mathbb{F}_q[x]$ with $i > j \geq 1$, $0 \neq a$, and assume that $\text{g.c.d.}(i-j, q-1) = 1$. Then f permutes \mathbb{F}_q if and only if $b = 0$ and $\text{g.c.d.}(i, q-1) = 1$.

Definition 1.20. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be in **normalized form** (or **reduced form**) if and only if the following statements hold:

- (1) f is monic, i.e. the leading coefficient of f is 1,
- (2) $f(0) = 0$, and
- (3) the coefficient of x^{m-1} is 0 when m is the degree of f and $p \nmid m$.

Note that any permutation polynomial can be put into normalized form.

Example 1.21. $f(x) = x^5 + 2x^3 + 2x^2 + x \in \mathbb{F}_3[x]$ is in normalized form but it is not a permutation polynomial of \mathbb{F}_3 since $f(0) = 0 = f(1)$.

Definition 1.22. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be a **normalized permutation polynomial** of \mathbb{F}_q if and only if f is a permutation polynomial of \mathbb{F}_q and f is in normalized form.

Example 1.23. Let $f(x) = x^3 - 2x \in \mathbb{F}_3[x]$. Then f is in normalized form. Also by Lemma 1.8 f is a permutation polynomial of \mathbb{F}_3 . Hence f is a normalized permutation polynomial of \mathbb{F}_3 .

On the basis of Hermite-Dickson's criterion, the following list of all normalized permutation polynomials of degree ≤ 5 (Table A) is tabulated in [1] and [5].

Table A

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

The next set of theorems taken from [5], [6] and [7] provide further classes of permutation polynomials.

Theorem 1.24. *Let $r \in \mathbb{N}$ with $\text{g.c.d.}(r, q - 1) = 1$ and let s be a positive divisor of $q - 1$. Let $g \in \mathbb{F}_q[x]$ be such that $g(x^s)$ has no nonzero root in \mathbb{F}_q . Then $f(x) = x^r(g(x^s))^{(q-1)/s}$ is a permutation polynomial of \mathbb{F}_q .*

Theorem 1.25. Let $f(x) = ax^i + bx^j + c \in \mathbb{F}_q[x]$ with $a \neq 0$ and $i > j \geq 1$. Assume that $-ba^{-1}$ is an $(i - j)^{\text{th}}$ power in \mathbb{F}_q . Then f permutes \mathbb{F}_q if and only if $b = 0$ and $\text{g.c.d.}(i, q - 1) = 1$.

Theorem 1.26. Let $f(x) = ax^i + bx^j + c \in \mathbb{F}_q[x]$ with $i > j \geq 1$, $a \neq 0$, $j \mid i$, $\text{g.c.d.}(\frac{i}{j} - 1, q - 1) = d$, and $\text{g.c.d.}(j, q - 1) = 1$. Suppose $-ba^{-1}\beta^{-1}$ is a d^{th} power in \mathbb{F}_q , where $\beta = z^{(i/j)-1} + z^{(i/j)-2} + \dots + 1$ for some $z \in \mathbb{F}_q$ and $z \neq 1$. Then f permutes \mathbb{F}_q if and only if $b = 0$ and $\text{g.c.d.}(i, q - 1) = 1$.

Theorem 1.27. If $f(x) = ax^k + bx^{k-2} + c$, where $a \neq 0$ and $k \geq 2$, permutes \mathbb{F}_q , then $q \not\equiv \pm 1 \pmod{k}$ or $b = 0$.

Theorem 1.28. Let $f(x) = x^i - ax^j$, $i > j \geq 1$, $0 \neq a \in \mathbb{F}_q$, and put $k = i - j$. Assume f permutes \mathbb{F}_q and suppose without loss of generality that $i < q - 1$ and $k \geq 2$. Then either $i \nmid q - 1 + k$, or $\frac{q-1+k}{i}$ is a multiple of p , the characteristic of \mathbb{F}_q . The second case cannot arise unless $p \mid k - 1$.

Theorem 1.29. Let $f(x) = x^{p^s} - ax^{p^r}$ where $s > r \geq 0$, $0 \neq a \in \mathbb{F}_q$. Then

- (1) f permutes \mathbb{F}_q if and only if a is not a $(p^s - p^r)^{\text{th}}$ power in \mathbb{F}_q ;
- (2) If a is a primitive element in \mathbb{F}_q (i.e., a generator for the multiplicative group \mathbb{F}_q^*), then f permutes \mathbb{F}_q , unless $p = 2$ and $\text{g.c.d.}(s - r, n) = 1$ where $q = p^n$.

The objectives of this thesis are as follows:

- (i) to determine all normalized permutation polynomials of degree 6 over fields whose characteristics are relatively prime to 6,
- (ii) to find new classes of permutation polynomials.

These two kinds of problems are posed in [3] and [4] and the results are shown in Chapters II and III.

CHAPTER II

NORMALIZED PERMUTATION POLYNOMIALS OF DEGREE 6

In this chapter, we will use Theorem 1.11 and ideas from [2] in order to determine all normalized permutation polynomials of degree 6 over \mathbb{F}_q where q is relatively prime to 6.

At first, we shall state a *Multinomial Theorem* that will be later used .

Multinomial Theorem: *Let R be a commutative ring with identity, n a positive integer, and $a_1, a_2, \dots, a_s \in R$. Then*

$$(a_1 + a_2 + \dots + a_s)^n = \sum \frac{n!}{i_1! i_2! \dots i_s!} a_1^{i_1} a_2^{i_2} \dots a_s^{i_s},$$

where the sum is over all s -tuples of nonnegative integers (i_1, i_2, \dots, i_s) such that $i_1 + i_2 + \dots + i_s = n$.

Consider the general polynomial of degree 6 over \mathbb{F}_q , $\text{g.c.d.}(q, 6) = 1$, $q = p^n$, $ax^6 + bx^5 + cx^4 + dx^3 + ex^2 + rx + s$. Its normalized form is the form $f(x) = x^6 + cx^4 + dx^3 + ex^2 + rx$.

It is enough to consider $q > 6$ (else degree of $f(x) \pmod{x^q - x} < 6$).

Since $q = p^n$ is relatively prime to 6, $q = 6m + 1$ or $6m + 5$ for some $m \in \mathbb{Z}^+$. If $q = 6m + 1$, then by Corollary 1.12, $f(x)$ is not a permutation polynomial of \mathbb{F}_q . Hence $q = 6m + 5$.

Clearly, $m + 1 < 6m + 4 = q - 1$.

If $m + 1 \equiv 0 \pmod{p}$, then $p \mid (m + 1)$, so $p \mid (p^n + 1)$ since $p^n + 1 = q + 1 = 6(m + 1)$, and then $p \mid 1$, a contradiction. Hence $m + 1 \not\equiv 0 \pmod{p}$.

Consider

$$\begin{aligned}
(f(x))^{m+1} &= (x^6 + cx^4 + dx^3 + ex^2 + rx)^{m+1} \\
&= x^{6(m+1)} + \binom{m+1}{1} x^{6m} (cx^4 + dx^3 + ex^2 + rx) \\
&\quad + \binom{m+1}{2} x^{6m-6} (cx^4 + dx^3 + ex^2 + rx)^2 \\
&\quad + \cdots + (cx^4 + dx^3 + ex^2 + rx)^{m+1}.
\end{aligned}$$

Then the coefficient of x^{6m+4} in $(f(x))^{m+1} \pmod{x^q - x}$ is $(m+1)c$. By Theorem 1.11, $(m+1)c = 0$. Since $m+1 \not\equiv 0 \pmod{p}$, $c = 0$. Hence $f(x) = x^6 + dx^3 + ex^2 + rx$.

Clearly, $m+2 < 6m+4 = q-1$.

If $p = 7 = 6 + 1$, then $q = p^n = 7^n \equiv 1 \pmod{6}$, a contradiction. Thus $p \neq 7$. To prove that $m+2 \not\equiv 0 \pmod{p}$, suppose not. Then $p \mid (m+2)$, so $p \mid (p^n + 7)$ since $p^n + 7 = q + 7 = 6(m+2)$. Then $p \mid 7$, so $p = 7$, a contradiction. Hence $m+2 \not\equiv 0 \pmod{p}$.

Consider

$$\begin{aligned}
(f(x))^{m+2} &= (x^6 + dx^3 + ex^2 + rx)^{m+2} \\
&= x^{6(m+2)} + \binom{m+2}{1} x^{6m+6} (dx^3 + ex^2 + rx) \\
&\quad + \binom{m+2}{2} x^{6m} (dx^3 + ex^2 + rx)^2 \\
&\quad + \binom{m+2}{3} x^{6m-6} (dx^3 + ex^2 + rx)^3 \\
&\quad + \cdots + (dx^3 + ex^2 + rx)^{m+2}.
\end{aligned}$$

By *Multinomial Theorem*, the coefficient of x^{6m+4} in $(f(x))^{m+2} \pmod{x^q - x}$ is $\binom{m+2}{2} (2dr + e^2) = \frac{(m+2)(m+1)}{2} (2dr + e^2)$. By Theorem 1.11, $\frac{(m+2)(m+1)}{2} (2dr + e^2) = 0$. Since $m+1 \not\equiv 0 \pmod{p}$ and $m+2 \not\equiv 0 \pmod{p}$, $\frac{(m+2)(m+1)}{2} \not\equiv 0 \pmod{p}$, so

$$2dr + e^2 = 0. \tag{2.1}$$

Clearly, $m + 3 < 6m + 4 = q - 1$.

If $p = 13 = 6(2) + 1$, then $q = p^n = 13^n \equiv 1 \pmod{6}$, a contradiction. Thus $p \neq 13$. To prove that $m + 3 \not\equiv 0 \pmod{p}$, suppose not. Then $p \mid (m + 3)$, so $p \mid (p^n + 13)$ since $p^n + 13 = q + 13 = 6(m + 3)$. Then $p \mid 13$, so $p = 13$, a contradiction. Hence $m + 3 \not\equiv 0 \pmod{p}$.

Consider

$$\begin{aligned}
(f(x))^{m+3} &= (x^6 + dx^3 + ex^2 + rx)^{m+3} \\
&= x^{6(m+3)} + \binom{m+3}{1} x^{6m+12} (dx^3 + ex^2 + rx) \\
&\quad + \binom{m+3}{2} x^{6m+6} (dx^3 + ex^2 + rx)^2 \\
&\quad + \binom{m+3}{3} x^{6m} (dx^3 + ex^2 + rx)^3 \\
&\quad + \binom{m+3}{4} x^{6m-6} (dx^3 + ex^2 + rx)^4 \\
&\quad + \binom{m+3}{5} x^{6m-12} (dx^3 + ex^2 + rx)^5 \\
&\quad + \cdots + (dx^3 + ex^2 + rx)^{m+3}.
\end{aligned}$$

Case 1. $m > 1$. Then $q = 6m+5 > 11$. By *Multinomial Theorem*, the coefficient of x^{6m+4} in $(f(x))^{m+3} \pmod{x^q - x}$ is $\binom{m+3}{3} \left[\frac{3!}{2!} er^2 \right] + \binom{m+3}{4} \left[\frac{4!}{3!} d^3 r + \frac{4!}{2!2!} d^2 e^2 \right] = \binom{m+3}{3} \left[3er^2 + \frac{m}{2}(2d^3 r + 3d^2 e^2) \right]$. By Theorem 1.11, $\binom{m+3}{3} \left[3er^2 + \frac{m}{2}(2d^3 r + 3d^2 e^2) \right] = 0$. Since $m + 1, m + 2, m + 3 \not\equiv 0 \pmod{p}$, $\binom{m+3}{3} \not\equiv 0 \pmod{p}$, so $\left[3er^2 + \frac{m}{2}(2d^3 r + 3d^2 e^2) \right] = 0$, i.e.

$$6er^2 + m(2d^3 r + 3d^2 e^2) = 0. \quad (2.2)$$

Clearly, $m + 4 < 6m + 4 = q - 1$.

If $p = 19 = 6(3) + 1$, then $q = p^n = 19^n \equiv 1 \pmod{6}$, a contradiction. Thus $p \neq 19$. To prove that $m + 4 \not\equiv 0 \pmod{p}$, suppose not. Then $p \mid (m + 4)$, so

$p \mid (p^n + 19)$ since $p^n + 19 = q + 19 = 6(m + 4)$. Then $p \mid 19$, so $p = 19$, a contradiction. Hence $m + 4 \not\equiv 0 \pmod{p}$.

Consider

$$\begin{aligned}
(f(x))^{m+4} &= (x^6 + dx^3 + ex^2 + rx)^{m+4} \\
&= x^{6(m+4)} + \binom{m+4}{1} x^{6m+18} (dx^3 + ex^2 + rx) + \cdots \\
&\quad + \binom{m+4}{4} x^{6m} (dx^3 + ex^2 + rx)^4 \\
&\quad + \binom{m+4}{5} x^{6m-6} (dx^3 + ex^2 + rx)^5 \\
&\quad + \binom{m+4}{6} x^{6m-12} (dx^3 + ex^2 + rx)^6 \\
&\quad + \binom{m+4}{7} x^{6m-18} (dx^3 + ex^2 + rx)^7 \\
&\quad + \cdots + (dx^3 + ex^2 + rx)^{m+4}.
\end{aligned}$$

Subcase 1.1. $m > 2$. Then $q = 6m + 5 > 17$. First note that if $p = 5$, then $5^n = p^n = q = 6m + 5$, so $5 \mid m$ and so $\frac{m}{5}$ is a positive integer. By *Multinomial Theorem*, the coefficient of x^{6m+4} in $(f(x))^{m+4} \pmod{x^q - x}$ is $\binom{m+4}{4} r^4 + \binom{m+4}{5} \left[\frac{5!}{2!2!} d^2 e r^2 + \frac{5!}{3!} d e^3 r + e^5 \right] + \binom{m+4}{6} \left[\frac{6!}{5!} d^5 r + \frac{6!}{4!2!} d^4 e^2 \right] = \binom{m+4}{4} \left[r^4 + \frac{m}{5} (30d^2 e r^2 + 20d e^3 r + e^5) + \frac{m(m-1)}{6 \cdot 5} (6d^5 r + 15d^4 e^2) \right]$. By Theorem 1.11, $\binom{m+4}{4} \left[r^4 + \frac{m}{5} (30d^2 e r^2 + 20d e^3 r + e^5) + \frac{m(m-1)}{6 \cdot 5} (6d^5 r + 15d^4 e^2) \right] = 0$. Since $m + 1, m + 2, m + 3, m + 4 \not\equiv 0 \pmod{p}$, $\binom{m+4}{4} \not\equiv 0 \pmod{p}$, so

$$r^4 + \frac{m}{5} (30d^2 e r^2 + 20d e^3 r + e^5) + \frac{m(m-1)}{6 \cdot 5} (6d^5 r + 15d^4 e^2) = 0. \quad (2.3)$$

From (2.1), we have $e^2 = -2dr$. Substituting into (2.2) and (2.3), we get

$$0 = 6er^2 + m[2d^3r + 3d^2(-2dr)] = 6er^2 - 4md^3r. \quad (2.4)$$

$$\begin{aligned}
0 &= r^4 + \frac{m}{5} [30d^2 e r^2 + 20d e r(-2dr) + e(4d^2 r^2)] \\
&\quad + \frac{m(m-1)}{6 \cdot 5} [6d^5 r + 15d^4(-2dr)] \\
&= r^4 - \frac{6m}{5} d^2 e r^2 - \frac{4m(m-1)}{5} d^5 r.
\end{aligned} \quad (2.5)$$

From (2.4), we have $6er^2 = 4md^3r$. Substituting into (2.5), we get

$$0 = r^4 - \frac{m}{5} d^2(4md^3r) - \frac{4m(m-1)}{5} d^5r = r^4 - \frac{4m(2m-1)}{5} d^5r. \quad (2.6)$$

Multiplying (2.1) by md^2 ,

$$2md^3r + md^2e^2 = 0. \quad (2.7)$$

Subtracting (2.7) from (2.2),

$$6er^2 + 2md^2e^2 = 0. \quad (2.8)$$

Next, we shall show that $e = 0$. Suppose not.

If $p = 5$, then $m \equiv 0 \pmod{p}$, so that from (2.8), $6er^2 = 0$, but since $6 \not\equiv 0 \pmod{5}$, $er^2 = 0$, then $r^2 = 0$ and so $r = 0$.

Assume that $p \neq 5$. Then from (2.8), $3r^2 + md^2e = 0$, and so $md^2e = -3r^2$.

Substituting into (2.5), we get

$$0 = r^4 - \frac{6}{5}r^2(-3r^2) - \frac{4m(m-1)}{5}d^5r = r^4 + \frac{18}{5}r^4 - \frac{4m(m-1)}{5}d^5r, \quad ,$$

and then

$$0 = 5\left(r^4 + \frac{18}{5}r^4 - \frac{4m(m-1)}{5}d^5r\right) = 23r^4 - 4m(m-1)d^5r. \quad (2.9)$$

If $2m-1 \equiv 0 \pmod{p}$, then $p \mid (2m-1)$, and so $p \mid (p^n - 8)$ since $p^n - 8 = 3(2m-1)$, and then $p \mid 8$, so $p = 2$, a contradiction. Hence $2m-1 \not\equiv 0 \pmod{p}$.

From (2.6), we have $4md^5r = \frac{5r^4}{2m-1}$. Substituting into (2.9), we get

$$0 = 23r^4 - (m-1)\left(\frac{5r^4}{2m-1}\right) = r^4\left(23 - \frac{5(m-1)}{2m-1}\right)$$

and so $0 = r^4[23(2m-1) - 5(m-1)] = r^4(41m - 18)$. Since $42m + 35 = 7(6m + 5) \equiv 0 \pmod{p}$, $41m \equiv (-35 - m) \pmod{p}$ and so $18r^4 = 41mr^4 =$

$(-35 - m)r^4 = -35r^4 - mr^4$ and then $mr^4 = -53r^4$. Thus $18r^4 = -2173r^4$, so $0 = 2191r^4 = 7 \cdot 313r^4$. Since $7 \not\equiv 0 \pmod{p}$, $313r^4 = 0$. To show that $313 \not\equiv 0 \pmod{p}$, suppose not. Since 313 is prime, $p = 313 = 6(52) + 1$, so $q = 313^n = 6k + 1$ for some $k \in \mathbb{Z}^+$, then $q \not\equiv 5 \pmod{6}$, a contradiction. Hence $313 \not\equiv 0 \pmod{p}$. Therefore $r^4 = 0$, i.e. $r = 0$.

Thus $r = 0$ for both $p = 5$ and $p \neq 5$. Substituting $r = 0$ into (2.1), we get $e^2 = 0$ and then $e = 0$, a contradiction.

Hence $e = 0$. By (2.1), $dr = 0$. Substituting into (2.6), we get $r^4 = 0$, so $r = 0$. Hence $f(x) = x^6 + dx^3$.

Clearly, $3m + 2 < 6m + 4 = q - 1$. Suppose that $3m + 2 \equiv 0 \pmod{p}$. Then $p \mid (3m + 2)$, so $p \mid (p^n - 1)$ since $p^n - 1 = 2(3m + 2)$. Thus $p \mid 1$, a contradiction. Hence $3m + 2 \not\equiv 0 \pmod{p}$.

Consider

$$\begin{aligned}
(f(x))^{3m+2} &= (x^6 + dx^3)^{3m+2} \\
&= x^{9m+6}(x^3 + d)^{3m+2} \\
&= x^{9m+6} [(x^3)^{3m+2} + a_{3m+1}(x^3)^{3m+1} + \dots + a_i(x^3)^i \\
&\quad + \dots + a_1(x^3) + a_0] \\
&= x^{3(6m+4)} + a_{3m+1}x^{9m+6+3(3m+1)} + a_{3m}x^{9m+6+3(3m)} \\
&\quad + \dots + a_i x^{9m+6+3i} + \dots + a_0 x^{9m+6}
\end{aligned}$$

where a_i is the coefficient of $(x^3)^i$ in $(x^3 + d)^{3m+2}$, $0 \leq i \leq 3m + 1$.

Claim that for all integer i , $0 \leq i \leq 3m + 1$ implies $x^{9m+6+3i} \not\equiv x^{6m+4} \pmod{x^{6m+5} - x}$. Since $x^{z(6m+4)} \equiv x^{6m+4} \pmod{x^{6m+5} - x}$ for all integer z , it suffices to show that $9m + 6 + 3i \not\equiv 0 \pmod{6m + 4}$ for each integer i where $0 \leq i \leq 3m + 1$.

Let i be an integer such that $0 \leq i \leq 3m + 1$. Then $0 < 8 < 3m + 2 \leq i + 3m + 2 \leq 6m + 3 < 6m + 4$. Suppose that $9m + 6 + 3i \equiv 0 \pmod{6m + 4}$. Then $9m + 6 + 3i = (6m + 4)w$ for some $w \in \mathbb{Z}^+$, and so $3(i + 3m + 2) = (6m + 4)w$. Since 3 is prime and $3 \nmid (6m + 4)$, $3 \mid w$, so $w = 3u$ for some $u \in \mathbb{Z}^+$. Thus $i + 3m + 2 = (6m + 4)u \equiv 0 \pmod{6m + 4}$, a contradiction, and the claim is proved. Therefore the coefficient of x^{6m+4} in $(f(x))^{3m+2} \pmod{x^q - x}$ is $1 \neq 0$. Hence for $m > 2$, there is no permutation polynomial of degree 6 over \mathbb{F}_q .

Subcase 1.2. $m = 2$. Then $q = 6(2) + 5 = 17$, so $p = 17$.

Consider

$$\begin{aligned}
(f(x))^{m+4} &= (f(x))^6 \\
&= (x^6 + dx^3 + ex^2 + rx)^6 \\
&= x^6(x^5 + dx^2 + ex + r)^6 \\
&= x^6(x^{30} + a_{29}x^{29} + \cdots + a_1x + a_0) \\
&\equiv x^4 + a_{29}x^3 + a_{28}x^2 + a_{27}x + a_{26}x^{16} + a_{25}x^{15} + \cdots + a_{11}x \\
&\quad + a_{10}x^{16} + a_9x^{15} + \cdots + a_1x^7 + a_0x^6 \pmod{x^{17} - x}
\end{aligned}$$

where a_i is the coefficient of x^i in $(x^5 + dx^2 + ex + r)^6$.

By *Multinomial Theorem*, $a_{26} = \frac{6!}{5!}e = 6e$ and $a_{10} = \frac{6!}{4!2!}r^4 + \frac{6!}{2!2!}d^2er^2 + \frac{6!}{3!}de^3r + \frac{6!}{5!}d^5r + \frac{6!}{5!}e^5 + \frac{6!}{4!2!}d^4e^2 = 15r^4 + 180d^2er^2 + 120de^3r + 6d^5r + 6e^5 + 15d^4e^2 = 15r^4 + 10d^2er^2 + de^3r + 6d^5r + 6e^5 + 15d^4e^2$. Hence the coefficient of x^{16} in $(f(x))^6 \pmod{x^{17} - x}$ is $6e + 15r^4 + 10d^2er^2 + de^3r + 6d^5r + 6e^5 + 15d^4e^2$.

By Theorem 1.11,

$$6e + 15r^4 + 10d^2er^2 + de^3r + 6d^5r + 6e^5 + 15d^4e^2 = 0. \quad (2.10)$$

Since $2 \not\equiv 0 \pmod{17}$, by (2.2),

$$3er^2 + 2d^3r + 3d^2e^2 = 0. \quad (2.11)$$

From (2.1), we get $e^2 = -2dr$. Substituting into (2.10) and (2.11), we get

$$0 = 3er^2 + 2d^3r + 3d^2(-2dr) = 3er^2 - 4d^3r \quad (2.12)$$

and

$$\begin{aligned} 0 &= 6e + 15r^4 + 10d^2er^2 + der(-2dr) + 6d^5r + 6e(4d^2r^2) + 15d^4(-2dr) \\ &= 6e + 15r^4 + 10d^2er^2 - 2d^2er^2 + 6d^5r + 24d^2er^2 - 30d^5r \\ &= 6e + 15r^4 + 32d^2er^2 - 24d^5r \\ &= 6e + 15r^4 - 36d^2er^2 - 24d^5r \\ &= 3(2e + 5r^4 - 12d^2er^2 - 8d^5r). \end{aligned}$$

Since $3 \not\equiv 0 \pmod{17}$,

$$0 = 2e + 5r^4 - 12d^2er^2 - 8d^5r. \quad (2.13)$$

From (2.12), $3er^2 = 4d^3r$. Substituting into (2.13), we get

$$0 = 2e + 5r^4 - 12d^2er^2 - 2d^2(3er^2) = 2e + 5r^4 - d^2er^2. \quad (2.14)$$

To show that $e = 0$, suppose not. From (2.1), $e^2 = -2dr$, so $d \neq 0$ and $r \neq 0$. Then from (2.11) and $3er^2 = 4d^3r$,

$$\begin{aligned} 0 &= 3er^2 + \frac{3er^2}{2} + 3d^2e^2 \\ &= 3er^2 - 7er^2 + 3d^2e^2 \\ &= -4er^2 + 3d^2e^2 \\ &= e(-4r^2 + 3d^2e), \end{aligned}$$

so $0 = -4r^2 + 3d^2e,$

and so $r^2 = \frac{3d^2e}{4} = \frac{-14d^2e}{4} = \frac{10d^2e}{2} = 5d^2e$. Substituting into (2.14), we have $0 = 2e + 5(25d^4e^2) - d^2e(5d^2e) = 2e + d^4e^2 = 2e + d^4(-2dr) = 2e - 2d^5r$ and so $0 = e - d^5r$. Then $e = d^5r$. Since $3er^2 = 4d^3r$, $3d^5r^3 = 3er^2 = 4d^3r$. Since $d \neq 0$ and $r \neq 0$, $3d^2r^2 = 4$, then $e^4 = 4d^2r^2 = \frac{16}{3} = \frac{-18}{3} = -6$, so $e^{q-1} = e^{16} = (-6)^4 = 4 \neq 1$, a contradiction. Hence $e = 0$. From (2.14), $5r^4 = 0$ and so $r = 0$. Therefore $f(x) = x^6 + dx^3$.

If $d = 0$, then $f(x) = x^6$ and since $\text{g.c.d.}(6, 17 - 1) = 2 \neq 1$, $f(x)$ is not a permutation polynomial of \mathbb{F}_{17} .

If $d \neq 0$, then by Proposition 1.19, $f(x) = x^6 + dx^3$ is not a permutation polynomial of \mathbb{F}_{17} .

Hence there is no permutation polynomial of degree 6 over \mathbb{F}_{17} .

Case 2. $m = 1$. That is $q = 6(1) + 5 = 11$. From above, we get $f(x) = x^6 + dx^3 + ex^2 + rx$. For each integer t with $3 \leq t \leq q - 2 = 9$, consider $(f(x))^t = x^t(x^5 + dx^2 + ex + r)^t$.

If $t = 3$, then by *Multinomial Theorem*, the coefficient of x^{10} in $(f(x))^t \pmod{x^{11} - x}$ is $3!dr + \frac{3!}{2!}e^2 = 6dr + 3e^2$, and by Theorem 1.11, $6dr + 3e^2 = 0$, and so

$$2dr + e^2 = 0. \quad (2.15)$$

If $t = 4$, then by *Multinomial Theorem* and $x^{20} = x^{11} \cdot x^9 \equiv x^{10} \pmod{x^{11} - x}$, the coefficient of x^{10} in $(f(x))^t \pmod{x^{11} - x}$ is $\frac{4!}{3!}e + \frac{4!}{2!}er^2 + \frac{4!}{3!}d^3r + \frac{4!}{2!2!}d^2e^2 = 4e + 12er^2 + 4d^3r + 6d^2e^2$, and by Theorem 1.11, $4e + 12er^2 + 4d^3r + 6d^2e^2 = 0$, and so

$$2e + 6er^2 + 2d^3r + 3d^2e^2 = 0. \quad (2.16)$$

If $t = 5$, then by *Multinomial Theorem* and $x^{20} = x^{11} \cdot x^9 \equiv x^{10} \pmod{x^{11} - x}$ and $x^{30} = x^{11} \cdot x^{11} \cdot x^8 \equiv x^{10} \pmod{x^{11} - x}$, the coefficient of x^{10} in $(f(x))^t \pmod{x^{11} - x}$

$x^{11} - x$) is $1 + \frac{5!}{3!2!}r^2 + \frac{5!}{2!2!}d^2e + \frac{5!}{4!}r^4 + \frac{5!}{2!2!}d^2er^2 + \frac{5!}{3!}de^3r + e^5 = 1 + 10r^2 + 30d^2e + 5r^4 + 30d^2er^2 + 20de^3r + e^5 = 1 + 10r^2 + 8d^2e + 5r^4 + 8d^2er^2 + 9de^3r + e^5$, and by Theorem 1.11,

$$1 + 10r^2 + 8d^2e + 5r^4 + 8d^2er^2 + 9de^3r + e^5 = 0. \quad (2.17)$$

If $t = 6$, then by *Multinomial Theorem* and $x^{20} = x^{11} \cdot x^9 \equiv x^{10} \pmod{x^{11} - x}$ and $x^{30} = x^{11} \cdot x^{11} \cdot x^8 \equiv x^{10} \pmod{x^{11} - x}$, the coefficient of x^{10} in $(f(x))^t \pmod{x^{11} - x}$ is $\frac{6!}{4!2!}d^2 + \frac{6!}{2!2!2!}d^2r^2 + \frac{6!}{2!2!}de^2r + \frac{6!}{2!4!}e^4 + \frac{6!}{4!}d^4e + \frac{6!}{4!2!}d^2r^4 + \frac{6!}{3!2!}de^2r^3 + \frac{6!}{4!2!}e^4r^2 = 4d^2 + 2d^2r^2 + 4de^2r + 4e^4 + 8d^4e + 4d^2r^4 + 5de^2r^3 + 4e^4r^2$, and by Theorem 1.11,

$$4d^2 + 2d^2r^2 + 4de^2r + 4e^4 + 8d^4e + 4d^2r^4 + 5de^2r^3 + 4e^4r^2 = 0. \quad (2.18)$$

If $t = 7$, then by *Multinomial Theorem* and $x^{20} = x^{11} \cdot x^9 \equiv x^{10} \pmod{x^{11} - x}$, $x^{30} = x^{11} \cdot x^{11} \cdot x^8 \equiv x^{10} \pmod{x^{11} - x}$ and $x^{40} = x^{11} \cdot x^{11} \cdot x^{11} \cdot x^7 \equiv x^{10} \pmod{x^{11} - x}$, the coefficient of x^{10} in $(f(x))^t \pmod{x^{11} - x}$ is $\frac{7!}{4!}der + \frac{7!}{4!3!}e^3 + \frac{7!}{3!4!}d^4 + \frac{7!}{2!3!}der^3 + \frac{7!}{2!3!2!}e^3r^2 + \frac{7!}{4!2!}d^4r^2 + \frac{7!}{3!2!}d^3e^2r + \frac{7!}{2!4!}d^2e^4 + \frac{7!}{6!}d^6e + \frac{7!}{5!}der^5 + \frac{7!}{3!4!}e^3r^4 = der + 2e^3 + 2d^4 + 2der^3 + e^3r^2 + 6d^4r^2 + 2d^3e^2r + 6d^2e^4 + 7d^6e + 9der^5 + 2e^3r^4$, and by Theorem 1.11,

$$0 = der + 2e^3 + 2d^4 + 2der^3 + e^3r^2 + 6d^4r^2 + 2d^3e^2r + 6d^2e^4 + 7d^6e + 9der^5 + 2e^3r^4. \quad (2.19)$$

If $t = 8$, then by *Multinomial Theorem* and $x^{20} = x^{11} \cdot x^9 \equiv x^{10} \pmod{x^{11} - x}$, $x^{30} = x^{11} \cdot x^{11} \cdot x^8 \equiv x^{10} \pmod{x^{11} - x}$ and $x^{40} = x^{11} \cdot x^{11} \cdot x^{11} \cdot x^7 \equiv x^{10} \pmod{x^{11} - x}$, the coefficient of x^{10} in $(f(x))^t \pmod{x^{11} - x}$ is $\frac{8!}{6!}dr + \frac{8!}{6!2!}e^2 + \frac{8!}{4!3!}dr^3 + \frac{8!}{4!2!2!}e^2r^2 + \frac{8!}{3!3!}d^3er + \frac{8!}{3!2!3!}d^2e^3 + \frac{8!}{2!6!}d^6 + \frac{8!}{2!5!}dr^5 + \frac{8!}{2!2!4!}e^2r^4 + \frac{8!}{3!3!}d^3er^3 + \frac{8!}{2!3!2!}d^2e^3r^2 + \frac{8!}{6!2!}d^6r^2 + \frac{8!}{5!}de^5r + \frac{8!}{5!2!}d^5e^3r + \frac{8!}{7!}e^7 + \frac{8!}{4!4!}d^4e^4 + \frac{8!}{7!}dr^7 + \frac{8!}{2!6!}e^2r^6 = dr + 6e^2 + 5dr^3 + 2e^2r^2 + 9d^3er + 10d^2e^3 + 6d^6 + 3dr^5 + 2e^2r^4 + 9d^3er^3 + 8d^2e^3r^2 +$

$6d^6r^2 + 6de^5r + 3d^5e^2r + 8e^7 + 4d^4e^4 + 8dr^7 + 6e^2r^6$, and by Theorem 1.11,

$$\begin{aligned}
0 &= dr + 6e^2 + 5dr^3 + 2e^2r^2 + 9d^3er + 10d^2e^3 + 6d^6 + 3dr^5 \\
&\quad + 2e^2r^4 + 9d^3er^3 + 8d^2e^3r^2 + 6d^6r^2 + 6de^5r + 3d^5e^2r \\
&\quad + 8e^7 + 4d^4e^4 + 8dr^7 + 6e^2r^6. \tag{2.20}
\end{aligned}$$

If $t = 9$, then by *Multinomial Theorem* and $x^{20} = x^{11} \cdot x^9 \equiv x^{10} \pmod{x^{11} - x}$, $x^{30} = x^{11} \cdot x^{11} \cdot x^8 \equiv x^{10} \pmod{x^{11} - x}$, $x^{40} = x^{11} \cdot x^{11} \cdot x^{11} \cdot x^7 \equiv x^{10} \pmod{x^{11} - x}$ and $x^{50} = x^{11} \cdot x^{11} \cdot x^{11} \cdot x^{11} \cdot x^6 \equiv x^{10} \pmod{x^{11} - x}$, the coefficient of x^{10} in $(f(x))^t \pmod{x^{11} - x}$ is $\frac{9!}{8!}e + \frac{9!}{6!2!}er^2 + \frac{9!}{5!3!}d^3r + \frac{9!}{5!2!2!}d^2e^2 + \frac{9!}{4!4!}er^4 + \frac{9!}{3!3!3!}d^3r^3 + \frac{9!}{3!2!2!2!}d^2e^2r^2 + \frac{9!}{3!4!}de^4r + \frac{9!}{2!5!}d^5er + \frac{9!}{3!6!}e^6 + \frac{9!}{2!4!3!}d^4e^3 + \frac{9!}{8!}d^8 + \frac{9!}{2!6!}er^6 + \frac{9!}{3!5!}d^3r^5 + \frac{9!}{2!2!4!}d^2e^2r^4 + \frac{9!}{4!3!}de^4r^3 + \frac{9!}{5!3!}d^5er^3 + \frac{9!}{6!2!}e^6r^2 + \frac{9!}{4!3!2!}d^4e^3r^2 + \frac{9!}{3!5!}d^3e^5r + \frac{9!}{2!7!}d^2e^7 + \frac{9!}{8!}er^8 = 9e + 10er^2 + 9d^3r + 8d^2e^2 + 3er^4 + 8d^3r^3 + 3d^2e^2r^2 + de^4r + 5d^5er + 7e^6 + 6d^4e^3 + 9d^8 + 10er^6 + 9d^3r^5 + 7d^2e^2r^4 + de^4r^3 + 9d^5er^3 + 10e^6r^2 + 6d^4e^3r^2 + 9d^3e^5r + 3d^2e^7 + 9er^8$, and by Theorem 1.11,

$$\begin{aligned}
0 &= 9e + 10er^2 + 9d^3r + 8d^2e^2 + 3er^4 + 8d^3r^3 \\
&\quad + 3d^2e^2r^2 + de^4r + 5d^5er + 7e^6 + 6d^4e^3 + 9d^8 \\
&\quad + 10er^6 + 9d^3r^5 + 7d^2e^2r^4 + de^4r^3 + 9d^5er^3 \\
&\quad + 10e^6r^2 + 6d^4e^3r^2 + 9d^3e^5r + 3d^2e^7 + 9er^8. \tag{2.21}
\end{aligned}$$

In \mathbb{F}_{11} , the possible values of e^2 are 0, 1, 3, 4, 5 and 9.

Table showing all possible values of $-2dr$

$d \ r$	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	9	7	5	3	1	10	8	6	4	2
2	0	7	3	10	6	2	9	5	1	8	4
3	0	5	10	4	9	3	8	2	7	1	6
4	0	3	6	9	1	4	7	10	2	5	8
5	0	1	2	3	4	5	6	7	8	9	10
6	0	10	9	8	7	6	5	4	3	2	1
7	0	8	5	2	10	7	4	1	9	6	3
8	0	6	1	7	2	8	3	9	4	10	5
9	0	4	8	1	5	9	2	6	10	3	7
10	0	2	4	6	8	10	1	3	5	7	9

From (2.15), $e^2 = -2dr$, so the possible values of (d, r) or (r, d) are

$(0, 0), (0, 1), (0, 2), (0, 3), \dots, (0, 10),$

$(1, 1), (1, 3), (1, 4), (1, 5), (1, 9),$

$(2, 2), (2, 6), (2, 7), (2, 8), (2, 10),$

$(3, 3), (3, 4), (3, 5), (3, 9),$

$(4, 4), (4, 5), (4, 9),$

$(5, 5), (5, 9),$

$(6, 6), (6, 7), (6, 8), (6, 10),$

$(7, 7), (7, 8), (7, 10),$

$(8, 8), (8, 10),$

$(9, 9),$

$(10, 10).$

If $r = 0$, then from (2.15), $e = 0$. Substituting into (2.17), we get $0 = 1$, a contradiction. Hence $r \neq 0$.

Subcase 2.1. $d = 0$. From (2.15), we get $e = 0$. Substituting into (2.17), we get $0 = 1 + 10r^2 + 5r^4 = 1 - r^2 - 6r^4 = (1 - 3r^2)(1 + 2r^2) = (1 - 3r^2)(1 - 9r^2) = (1 - 3r^2)(1 - 3r)(1 + 3r)$, so $r^2 = \frac{1}{3} = \frac{12}{3} = 4$ or $r = \frac{1}{3} = \frac{12}{3} = 4$ or $r = \frac{-1}{3} = \frac{-12}{3} = -4$. Hence $r = \pm 2, \pm 4$ satisfying (2.15) to (2.21). Therefore $x^6 \pm 2x$ and $x^6 \pm 4x$ are permutation polynomials of \mathbb{F}_{11} .

Subcase 2.2. $d = 1$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 6er^2 + 3d^2e^2 - d^2e^2 = 2e + 6er^2 + 2e^2$, so $0 = 1 + 3r^2 + e$.

If $r = 1$, then $e = -4 = 7$ and (2.17) is not satisfied.

If $r = 3$, then $e = -6 = 5$ and (2.17) is not satisfied.

If $r = 4$, then $e = -16 = 6$ which satisfies (2.15) to (2.21).

If $r = 5$, then $e = -10 = 1$ which satisfies (2.15) to (2.21).

If $r = 9$, then $e = -13 = -2 = 9$ and (2.17) is not satisfied.

Hence $x^6 + x^3 + x^2 + 5x$ and $x^6 + x^3 + 6x^2 + 4x$ are permutation polynomials of \mathbb{F}_{11} .

Subcase 2.3. $r = 1$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 2d^2e^2 + 6e$, so $0 = 1 + d^2e + 3 = 4 + d^2e$.

If $d = 1$, then $e = -4 = 7$ and (2.17) is not satisfied.

If $d = 3$, then $e = \frac{-4}{9} = \frac{-4}{-2} = 2$ and (2.17) is not satisfied.

If $d = 4$, then $e = \frac{-4}{5} = \frac{4}{6} = \frac{2}{3} = \frac{-9}{3} = -3 = 8$ and (2.17) is not satisfied.

If $d = 5$, then $e = \frac{-4}{3} = \frac{-4}{-8} = \frac{1}{2} = \frac{-10}{2} = -5 = 6$ and (2.17) is not satisfied.

If $d = 9$, then $e = \frac{-4}{4} = -1 = 10$ and (2.17) is not satisfied.

Hence there is no permutation polynomials of \mathbb{F}_{11} in this case.

Subcase 2.4. $d = 2$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 8e^2 + 6er^2$, so $0 = 1 + 4e + 3r^2$.

If $r = 2$, then $e = \frac{-13}{4} = \frac{-2}{4} = \frac{-1}{2} = \frac{10}{2} = 5$ and (2.17) is not satisfied.

If $r = 6$, then $e = \frac{-10}{4} = \frac{-5}{2} = \frac{6}{2} = 3$ which satisfies (2.15) to (2.21).

If $r = 7$, then $e = \frac{-5}{4} = \frac{6}{4} = \frac{3}{2} = \frac{-8}{2} = -4 = 7$ which satisfies (2.15) to (2.21).

If $r = 8$, then $e = \frac{5}{4} = \frac{-3}{2} = \frac{8}{2} = 4$ and (2.17) is not satisfied.

If $r = 10$, then $e = \frac{-4}{4} = -1 = 10$ and (2.17) is not satisfied.

Hence $x^6 + 2x^3 + 3x^2 + 6x$ and $x^6 + 2x^3 + 7x^2 + 7x$ are permutation polynomials of \mathbb{F}_{11} .

Subcase 2.5. $r = 2$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 2d^2e^2 + 2e$, so $0 = 1 + d^2e + 1 = 2 + d^2e$.

If $d = 2$, then $e = \frac{-2}{4} = \frac{-1}{2} = \frac{10}{2} = 5$ and (2.17) is not satisfied.

If $d = 3$, then $e = \frac{-4}{9} = \frac{-4}{-2} = 2$ and (2.17) is not satisfied.

If $d = 6$, then $e = \frac{-2}{3} = \frac{9}{3} = 3$ and (2.17) is not satisfied.

If $d = 7$, then $e = \frac{-2}{5} = \frac{-2}{-6} = \frac{1}{3} = \frac{12}{3} = 4$ and (2.17) is not satisfied.

If $d = 8$, then $e = \frac{-2}{-2} = 1$ and (2.17) is not satisfied.

If $d = 10$, then $e = \frac{-2}{1} = -2 = 9$ and (2.17) is not satisfied.

Hence there is no permutation polynomials of \mathbb{F}_{11} in this case.

Subcase 2.6. $d = 3$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e - 4e^2 + 6er^2$, so $0 = 1 - 2e + 3r^2 = 1 + 9e + 3r^2$.

If $r = 3$, then $e = \frac{-6}{9} = \frac{-2}{3} = \frac{9}{3} = 3$ and (2.17) is not satisfied.

If $r = 4$, then $e = \frac{-5}{9} = \frac{6}{9} = \frac{6}{-2} = -3 = 8$ which satisfies (2.15) to (2.21).

If $r = 5$, then $e = \frac{-10}{9} = \frac{-10}{-2} = 5$ which satisfies (2.15) to (2.21).

If $r = 9$, then $e = \frac{-13}{9} = \frac{-2}{-2} = 1$ and (2.17) is not satisfied.

Hence $x^6 + 3x^3 + 8x^2 + 4x$ and $x^6 + 3x^3 + 5x^2 + 5x$ are permutation

polynomials of \mathbb{F}_{11} .

Subcase 2.7. $r = 3$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 2d^2e^2 + 10e$, so $0 = 1 + d^2e + 5 = 6 + d^2e$.

If $d = 3$, then $e = \frac{-6}{9} = \frac{-6}{-2} = 3$ and (2.17) is not satisfied.

If $d = 4$, then $e = \frac{-6}{-6} = 1$ and (2.17) is not satisfied.

If $d = 5$, then $e = \frac{-6}{3} = -2 = 9$ and (2.17) is not satisfied.

If $d = 9$, then $e = \frac{-6}{4} = \frac{-3}{2} = \frac{8}{2} = 4$ and (2.17) is not satisfied.

Hence there is no permutation polynomials of \mathbb{F}_{11} in this case.

Subcase 2.8. $d = 4$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 10e^2 + 6er^2$, so $0 = 1 + 5e + 3r^2$.

If $r = 4$, then $e = \frac{-5}{5} = -1 = 10$ which satisfies (2.15) to (2.21).

If $r = 5$, then $e = \frac{-10}{5} = -2 = 9$ which satisfies (2.15) to (2.21).

If $r = 9$, then $e = \frac{-2}{5} = \frac{20}{5} = 4$ and (2.17) is not satisfied.

Hence $x^6 + 4x^3 + 10x^2 + 4x$ and $x^6 + 4x^3 + 9x^2 + 5x$ are permutation polynomials of \mathbb{F}_{11} .

Subcase 2.9. $r = 4$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 2d^2e^2 + 8e$, so $0 = 1 + d^2e + 4 = 5 + d^2e$.

If $d = 4$, then $e = \frac{-5}{5} = -1 = 10$ which satisfies (2.15) to (2.21).

If $d = 5$, then $e = \frac{-5}{3} = \frac{6}{3} = 2$ which satisfies (2.15) to (2.21).

If $d = 9$, then $e = \frac{-5}{4} = \frac{6}{4} = \frac{3}{2} = \frac{-8}{2} = -4 = 7$ which satisfies (2.15) to (2.21).

Hence $x^6 + 4x^3 + 10x^2 + 4x$, $x^6 + 5x^3 + 2x^2 + 4x$ and $x^6 + 9x^3 + 7x^2 + 4x$ are permutation polynomials of \mathbb{F}_{11} .

Subcase 2.10. $d = 5$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 6e^2 + 6er^2$, so $0 = 1 + 3e + 3r^2$.

If $r = 5$, then $e = \frac{-10}{3} = \frac{1}{3} = \frac{12}{3} = 4$ which satisfies (2.15) to (2.21).

If $r = 9$, then $e = \frac{-2}{3} = \frac{9}{3} = 3$ and (2.17) is not satisfied.

Hence $x^6 + 5x^3 + 4x^2 + 5x$ is a permutation polynomial of \mathbb{F}_{11} .

Subcase 2.11. $r = 5$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 2d^2e^2 - 4e$, so $0 = 1 + d^2e - 2 = -1 + d^2e = 10 + d^2e$.

If $d = 5$, then $e = \frac{1}{3} = \frac{12}{3} = 4$ which satisfies (2.15) to (2.21).

If $d = 9$, then $e = \frac{1}{4} = \frac{-10}{4} = \frac{-5}{2} = \frac{6}{2} = 3$ which satisfies (2.15) to (2.21).

Hence $x^6 + 5x^3 + 4x^2 + 5x$, and $x^6 + 9x^3 + 3x^2 + 5x$ are permutation polynomials of \mathbb{F}_{11} .

Subcase 2.12. $d = 6$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 6e^2 + 6er^2$, so $0 = 1 + 3e + 3r^2$.

If $r = 6$, then $e = \frac{-10}{3} = \frac{12}{3} = 4$ which satisfies (2.15) to (2.21).

If $r = 7$, then $e = \frac{-5}{3} = \frac{6}{3} = 2$ which satisfies (2.15) to (2.21).

If $r = 8$, then $e = \frac{5}{3} = \frac{-6}{3} = -2 = 9$ and (2.17) is not satisfied.

If $r = 10$, then $e = \frac{-4}{3} = \frac{18}{3} = 6$ and (2.17) is not satisfied.

Hence $x^6 + 6x^3 + 4x^2 + 6x$ and $x^6 + 6x^3 + 2x^2 + 7x$ are permutation polynomials of \mathbb{F}_{11} .

Subcase 2.13. $r = 6$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 2d^2e^2 - 4e$, so $0 = 1 + d^2e - 2 = -1 + d^2e = 10 + d^2e$.

If $d = 6$, then $e = \frac{1}{3} = \frac{12}{3} = 4$ which satisfies (2.15) to (2.21).

If $d = 7$, then $e = \frac{1}{5} = \frac{-10}{5} = -2 = 9$ which satisfies (2.15) to (2.21).

If $d = 8$, then $e = \frac{1}{-2} = \frac{-10}{-2} = 5$ which satisfies (2.15) to (2.21).

If $d = 10$, then $e = \frac{1}{1} = 1$ which satisfies (2.15) to (2.21).

Hence $x^6 + 6x^3 + 4x^2 + 6x$, $x^6 + 7x^3 + 9x^2 + 6x$, $x^6 + 8x^3 + 5x^2 + 6x$ and $x^6 + 10x^3 + x^2 + 6x$ are permutation polynomials of \mathbb{F}_{11} .

Subcase 2.14. $d = 7$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 10e^2 + 6er^2$, so $0 = 1 + 5e + 3r^2$.

If $r = 7$, then $e = \frac{-5}{5} = -1 = 10$ which satisfies (2.15) to (2.21).

If $r = 8$, then $e = \frac{5}{5} = 1$ and (2.17) is not satisfied.

If $r = 10$, then $e = \frac{-4}{5} = \frac{-4}{-6} = \frac{2}{3} = \frac{-9}{3} = -3 = 8$ and (2.17) is not satisfied.

Hence $x^6 + 7x^3 + 10x^2 + 7x$ is a permutation polynomial of \mathbb{F}_{11} .

Subcase 2.15. $r = 7$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 2d^2e^2 + 8e$, so $0 = 1 + d^2e + 4 = 5 + d^2e$.

If $d = 7$, then $e = \frac{-5}{5} = -1 = 10$ which satisfies (2.15) to (2.21).

If $d = 8$, then $e = \frac{-5}{-2} = \frac{6}{-2} = -3 = 8$ which satisfies (2.15) to (2.21).

If $d = 10$, then $e = \frac{-5}{1} = -5 = 6$ which satisfies (2.15) to (2.21).

Hence $x^6 + 7x^3 + 10x^2 + 7x$, $x^6 + 8x^3 + 8x^2 + 7x$, and $x^6 + 10x^3 + 6x^2 + 7x$ are permutation polynomials of \mathbb{F}_{11} .

Subcase 2.16. $d = 8$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e - 4e^2 + 6er^2$, so $0 = 1 - 2e + 3r^2$.

If $r = 8$, then $e = \frac{5}{-2} = \frac{-6}{-2} = 3$ and (2.17) is not satisfied.

If $r = 10$, then $e = \frac{-4}{-2} = 2$ and (2.17) is not satisfied.

Hence there is no permutation polynomials of \mathbb{F}_{11} in this case.

Subcase 2.17. $r = 8$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 2d^2e^2 + 10e$, so $0 = 1 + d^2e + 5 = 6 + d^2e$.

If $d = 8$, then $e = \frac{5}{-2} = \frac{-6}{-2} = 3$ and (2.17) is not satisfied.

If $d = 10$, then $e = \frac{5}{1} = 5$ and (2.17) is not satisfied.

Hence there is no permutation polynomials of \mathbb{F}_{11} in this case.

Subcase 2.18. $d = 9$ and $r = 9$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 8e^2 + 2e = 4e + 8e^2$, so $0 = 1 + 2e$. Thus $e = \frac{-1}{2} = \frac{10}{2} = 5$

and (2.17) is not satisfied.

Hence there is no permutation polynomials of \mathbb{F}_{11} in this case.

Subcase 2.19. $d = 10$ and $r = 10$. Then $e \neq 0$. From (2.15) and (2.16), $0 = 2e + 3d^2e^2 - d^2e^2 + 6er^2 = 2e + 2e^2 + 6e = 8e + 2e^2$, so $0 = 4 + e$. Thus $e = -4 = 7$ and then (2.17) is not satisfied.

Hence there is no permutation polynomials of \mathbb{F}_{11} in this case.

Therefore for $m = 1$, all normalized permutation polynomials of \mathbb{F}_{11} of degree 6 are

$$x^6 \pm 2x,$$

$$x^6 \pm a^2x^3 + ax^2 \pm 5x \quad ; \quad a = 1, 3, 4, 5, 9,$$

$$x^6 \pm 4a^2x^3 + ax^2 \pm 4x \quad ; \quad a = 0, 2, 6, 7, 8, 10.$$

All normalized permutation polynomials of degree 6 over \mathbb{F}_q where q is relatively prime to 6 are shown in Table B.

Table B

Normalized permutation polynomials of \mathbb{F}_q	q
$x^6 \pm 2x$	$q = 11$
$x^6 \pm a^2x^3 + ax^2 \pm 5x \quad ; \quad a = 1, 3, 4, 5, 9$	$q = 11$
$x^6 \pm 4a^2x^3 + ax^2 \pm 4x \quad ; \quad a = 0, 2, 6, 7, 8, 10$	$q = 11$

CHAPTER III

SOME NEW CLASSES OF PERMUTATION POLYNOMIALS

In this chapter, we give some new results about permutation polynomials related to Theorem 1.24 - Theorem 1.29 stated in Chapter I.

The next two theorems are obtained by studying the proof of Theorem 1.24.

Theorem 3.1. *Let $r \in \mathbb{N}$ and s be a positive divisor of $q - 1$. Let $h, g \in \mathbb{F}_q[x]$ be such that $h(0) = 0$, $h(x^r)$ and $g(x^s)$ has no nonzero root in \mathbb{F}_q . If for each $t \in \mathbb{Z}$, $1 \leq t \leq q - 2$, the degree of each term in $h(x^r)^t$ is not divisible by s , then $f(x) = h(x^r)(g(x^s))^{(q-1)/s}$ is a permutation polynomial of \mathbb{F}_q .*

Proof. Assume that for each integer t , $1 \leq t \leq q - 2$, the degree of each term in $(h(x^r))^t$ is not divisible by s .

(1) We shall show that f has exactly one root in \mathbb{F}_q . Consider $f(x) = 0$. Then $h(x^r)(g(x^s))^{(q-1)/s} = 0$, so $h(x^r) = 0$ or $(g(x^s))^{(q-1)/s} = 0$. Then $x^r = 0$ or $g(x^s) = 0$. Since $g(x^s)$ and $h(x^r)$ has no nonzero root in \mathbb{F}_q , $x = 0$ is the only root of f .

(2) We shall show that for each integer t , $1 \leq t \leq q - 2$, the reduction of $(f(x))^t \pmod{x^q - x}$ has degree $\leq q - 2$.

Case 1. $s \mid t$, say $t = ks$ with $k \in \mathbb{N}$. Then $(f(x))^t = (h(x^r))^t (g(x^s))^{(q-1)k}$. Let $c \in \mathbb{F}_q^*$. Since $c^s \neq 0$ and $g(x^s)$ has no nonzero root in \mathbb{F}_q , $g(c^s) \neq 0$ and so $(g(c^s))^{q-1} = 1$. Thus $(f(c))^t = (h(c^r))^t (g(c^s))^{(q-1)k} = (h(c^r))^t$. Also since 0 is the only root of $h(x^r)$ in \mathbb{F}_q , $(f(0))^t = 0 = (h(0^r))^t$. By Lemma 1.9, $(f(x))^t \equiv h(x^r)^t \pmod{x^q - x}$. By assumption, each term in $(h(x^r))^t$ is of the form ax^{ru} where $s \nmid ru$ and a is a constant. Since $s \nmid ru$ and $s \mid (q - 1)$, $(q - 1) \nmid ru$, say

$ru = (q-1)A + \beta$ where $0 < \beta \leq q-2$. Thus $x^{ru} = x^{(q-1)A + \beta} = x^{qA - A + \beta} \equiv x^\beta \pmod{x^q - x}$. Hence the reduction of $(h(x^r))^t \pmod{x^q - x}$ has degree $\leq q-2$.

Case 2. $s \nmid t$. Then $(f(x))^t = (h(x^r))^t (g(x^s))^{(q-1)t/s}$. Each term in $(h(x^r))^t$ is of the form ax^{ru} . By assumption, $s \nmid ru$, so $(q-1) \nmid ru$. Hence $(f(x))^t$ is a sum of terms whose exponents are of the form $ru + sm$ where m is a nonnegative integer. Since $s \nmid ru$ and $s \mid sm$, $s \nmid (ru + sm)$. Then $(q-1) \nmid (ru + sm)$, say $ru + sm = (q-1)A + \beta$ where $0 < \beta \leq q-2$. Thus $x^{ru+sm} = x^{(q-1)A + \beta} = x^{qA - A + \beta} \equiv x^\beta \pmod{x^q - x}$. Hence the reduction of $(f(x))^t \pmod{x^q - x}$ has degree $\leq q-2$.

By Theorem 1.11, $f(x)$ is a permutation polynomial of \mathbb{F}_q . □

Theorem 3.2. *Let $r \in \mathbb{N}$ and s be a positive divisor of $q-1$ such that $\text{g.c.d.}(\frac{r(q-1)}{s}, s) = 1$ and $g \in \mathbb{F}_q[x]$ be such that $g(x^s)$ has root only at 0 in \mathbb{F}_q .*

Assume that for each integer t , $1 \leq t \leq q-2$, if $s \mid t$, then the reduction of $(g(x^s))^t \pmod{x^q - x}$ has degree $\leq q-2$. Then $f(x) = g(x^s)x^{r(q-1)/s}$ is a permutation polynomial of \mathbb{F}_q .

Proof. (1) We shall show that f has exactly one root in \mathbb{F}_q . Consider $f(x) = 0$. Then $g(x^s)x^{r(q-1)/s} = 0$. Since $g(x^s)$ has no nonzero root in \mathbb{F}_q , 0 is the only root of f .

(2) We shall show that for each integer t , $1 \leq t \leq q-2$, the reduction of $(f(x))^t \pmod{x^q - x}$ has degree $\leq q-2$.

Case 1. $s \mid t$, say $t = ks$ with $k \in \mathbb{N}$. Then $(f(x))^t = (g(x^s))^t x^{(q-1)rk}$. Let $c \in \mathbb{F}_q^*$. Then $(f(c))^t = (g(c^s))^t c^{(q-1)rk} = (g(c^s))^t$. And $(f(0))^t = (g(0^s))^t 0^{(q-1)rk} = 0 = (g(0^s))^t$. By Lemma 1.9, $(f(x))^t \equiv (g(x^s))^t \pmod{x^q - x}$. By assumption, the reduction of $(f(x))^t \pmod{x^q - x}$ has degree $\leq q-2$.

Case 2. $s \nmid t$. Then $(f(x))^t = (g(x^s))^t x^{(q-1)rt/s}$. Each term in $(g(x^s))^t$ is of the form ax^{su} . Thus $(f(x))^t$ is a sum of terms whose exponents are of the form $su + \frac{rt(q-1)}{s}$. If $(q-1) \mid (su + \frac{rt(q-1)}{s})$, then $su + \frac{rt(q-1)}{s} = (q-1)m$, so $s \mid \frac{rt(q-1)}{s}$, a

contradiction. Thus $(q-1) \nmid (su + \frac{rt(q-1)}{s})$, say $su + \frac{rt(q-1)}{s} = (q-1)A + \beta$ where $0 < \beta \leq q-2$. Then $x^{su + \frac{rt(q-1)}{s}} = x^{(q-1)A + \beta} = x^{qA - A + \beta} \equiv x^\beta \pmod{x^q - x}$. Hence the reduction of $(f(x))^t \pmod{x^q - x}$ has degree $\leq q-2$.

By Theorem 1.11, $f(x)$ is a permutation polynomial of \mathbb{F}_q . □

We now give examples of permutation polynomials of the form in Theorem 3.1 and Theorem 3.2 but not of the form in Theorem 1.24.

Example 3.3. Let $f(x) = x^{15} - 2x^3 \in \mathbb{F}_3[x]$, $h(x) = x^3 - 2x \in \mathbb{F}_3[x]$ and $g(x) = x^3 \in \mathbb{F}_3[x]$. Then $f(x) = (x^9 - 2x^3)x^6 = h(x^3)g(x^2)$, $g(x^2)$ and $h(x^3)$ has no nonzero root in \mathbb{F}_3 and $h(0) = 0$. Also the degree of each term in $h(x^3)$ is not divisible by 2. By Theorem 3.1, $f(x)$ is a permutation polynomial of \mathbb{F}_3 .

Example 3.4. Let $r \in \mathbb{N}$ and $f(x) = (x^3 + x^{3^2})x^{2r} = (x^3 + x^{3^2})x^{r(3-1)/1} \in \mathbb{F}_3[x]$, where $g(x) = x^3 + x^{3^2} \in \mathbb{F}_3[x]$. Clearly, $1 \mid q-1$ and $\text{g.c.d.}(2r, 1) = 1$. Since $g(0) = 0, g(1) = 2$ and $g(2) = 1$, $g(x)$ has only root at 0 in \mathbb{F}_3 and is a permutation polynomial of \mathbb{F}_3 , then for each integer $t, 1 \leq t \leq 3-2=1$, $(g(x))^t \equiv 2x \pmod{x^3 - x}$ which has degree $\leq 3-2=1$. By Theorem 3.2, $f(x)$ is a permutation polynomial of \mathbb{F}_3 .

Theorem 1.25 was proved by R.A.Mollin and C.Small in 1987 under an assumption on the coefficients. Removing this restriction we can still find a class of permutation polynomials.

Theorem 3.5. Let $f(x) = ax^i + bx^j + c, i > j \geq 1$ and $a(\neq 0), b, c \in \mathbb{F}_q$. Assume that $-ba^{-1}$ is not an $(i-j)^{\text{th}}$ power in \mathbb{F}_q . If $i-j = q-1$ and $\text{g.c.d.}(j, q-1) = 1$, then $f(x)$ is a permutation polynomial of \mathbb{F}_q .

Proof. Assume that $i-j = q-1$ and $\text{g.c.d.}(j, q-1) = 1$. By Proposition 1.14 we have that f permutes $\mathbb{F}_q \iff x^i + ba^{-1}x^j = x^j(x^{i-j} + ba^{-1})$ permutes \mathbb{F}_q . Since $\text{g.c.d.}(j, q-1) = 1, (i-j) \mid (q-1)$ and $-ba^{-1}$ is not an $(i-j)^{\text{th}}$ power in \mathbb{F}_q , by

Theorem 1.24, $x^j(x^{i-j} + ba^{-1})$ is a permutation polynomial of \mathbb{F}_q . Hence $f(x)$ is a permutation polynomial of \mathbb{F}_q . \square

Next, we give an example of Theorem 3.5.

Example 3.6. Let $f(x) = x^3 + x + c \in \mathbb{F}_3[x]$. We can show easily that -1 is not a square in \mathbb{F}_3 . By Theorem 3.5, $f(x)$ is a permutation polynomial of \mathbb{F}_3 .

Since the hypothesis on $-ba^{-1}\beta^{-1}$ in Theorem 1.26 is difficult to check, simplifying this condition, we get the following result.

Theorem 3.7. Let $f(x) = ax^i + bx^j + c$, $i > j \geq 1$, $a(\neq 0), b, c \in \mathbb{F}_q$, $j \mid i$ and $\text{g.c.d.}(j, q-1) = 1$. Then the following statements hold:

- (1) if $b = 0$, then f permutes $\mathbb{F}_q \iff \text{g.c.d.}(i, q-1) = 1$,
- (2) if $b \neq 0$, then $f(x)$ is not a permutation polynomial of \mathbb{F}_q provided that $x^{(i/j)-1} + ba^{-1}$ has a nonzero root in \mathbb{F}_q .

Proof. (1) Assume that $b = 0$. Then $f(x) = ax^i + c$. By Theorem 1.13 and Proposition 1.14, f permutes $\mathbb{F}_q \iff x^i$ permutes $\mathbb{F}_q \iff \text{g.c.d.}(i, q-1) = 1$.

(2) Assume that $b \neq 0$. Then $-ba^{-1} \neq 0$. By Lemma 1.18, $x^i + ba^{-1}x^j$ permutes $\mathbb{F}_q \iff x^{i/j} + ba^{-1}x = x(x^{(i/j)-1} + ba^{-1})$ permutes \mathbb{F}_q . If $x^{(i/j)-1} + ba^{-1}$ has a nonzero root β in \mathbb{F}_q , then $x(x^{(i/j)-1} + ba^{-1})$ has both 0 and $\beta \neq 0$ as roots in \mathbb{F}_q , so $x(x^{(i/j)-1} + ba^{-1})$ is not a permutation polynomial of \mathbb{F}_q . \square

In the case that $x^{(i/j)-1} + ba^{-1}$ has no nonzero root in \mathbb{F}_q , $f(x)$ may or may not be a permutation polynomial of \mathbb{F}_q as illustrated in the following examples.

Example 3.8. Let $f(x) = x^3 + 2x \in \mathbb{F}_5[x]$, i.e. $i = 3, j = 1, a = 1$, and $b = 2$. Then $x^{(i/j)-1} + ba^{-1} = x^2 + 2$ has no root in \mathbb{F}_5 and $f(x) = x(x^2 + 2)$. Since $f(1) = 3 = f(3)$, $f(x)$ is not one-to-one, so $f(x)$ is not a permutation polynomial of \mathbb{F}_5 .

Example 3.9. Let $f(x) = x^3 + x \in \mathbb{F}_3[x]$, i.e. $i = 3, j = 1, a = 1$, and $b = 1$. Then $x^{(i/j)-1} + ba^{-1} = x^2 + 1$ has no root in \mathbb{F}_3 and $f(x) = x(x^2 + 1)$. By Example 3.6, $f(x)$ is a permutation polynomial of \mathbb{F}_3 .

Theorem 1.27 was also proved by R.A.Mollin and C.Small in 1987. The following theorem is an extension of it.

Theorem 3.10. Let $f(x) = ax^k + bx^{k-2} + c \in \mathbb{F}_q[x]$ with $k \geq 2$ and $a \neq 0$. Then

- (1) For $q = 2$, f permutes $\mathbb{F}_q \iff b = 0$ or $k = 2$,
- (2) For $q = 3$, f permutes $\mathbb{F}_q \iff k$ is odd and either $b = 0$ or $ba^{-1} = 1$,
- (3) For $q > 3$,
 - (3.1) if f permutes \mathbb{F}_q , then either $b = 0$ or $q \not\equiv \pm 1 \pmod{k}$,
 - (3.2) assume that $x^2 + ba^{-1}$ has a root in \mathbb{F}_q . Then
 - (i) if $b = 0$, then f permutes $\mathbb{F}_q \iff g.c.d.(k, q - 1) = 1$,
 - (ii) if $b \neq 0$, then $k > 2$ implies $f(x)$ is not a permutation polynomial of \mathbb{F}_q while $k = 2$ implies \mathbb{F}_q has characteristic 2 $\iff f$ permutes \mathbb{F}_q .

Proof. (1) Let $q = 2$. Then

$$\begin{aligned}
 f \text{ permutes } \mathbb{F}_q &\iff x^k + ba^{-1}x^{k-2} \text{ permutes } \mathbb{F}_q \\
 &\iff x^{k-2}(x^2 + ba^{-1}) \text{ permutes } \mathbb{F}_q \\
 &\iff \text{either } b = 0 \text{ or } k = 2.
 \end{aligned}$$

(2) Let $q = 3$. We have

$$f \text{ permutes } \mathbb{F}_q \iff x^{k-2}(x^2 + ba^{-1}) \text{ permutes } \mathbb{F}_q.$$

Case 2.1 $b = 0$. Then

$$\begin{aligned} f \text{ permutes } \mathbb{F}_q &\iff x^k \text{ permutes } \mathbb{F}_q \\ &\iff g.c.d.(k, 2) = 1 \text{ (by Theorem 1.13), i.e. } k \text{ is odd.} \end{aligned}$$

Case 2.2 $b \neq 0$. If $ba^{-1} = 2$, then $h(x) = x^{k-2}(x^2 + ba^{-1}) = x^{k-2}(x^2 + 2)$ is not a permutation polynomial of \mathbb{F}_q since $h(1) = 0 = h(0)$, which implies that f is not a permutation polynomial of \mathbb{F}_q . Assume that $ba^{-1} = 1$. If $k = 2$, then $f(x) = ax^2 + b + c$ and $f(x)$ is not a permutation polynomial of \mathbb{F}_3 since $g.c.d.(2, 3 - 1) = 2 \neq 1$. Consider $k > 2$. Let $g(x) = x^{k-2}(x^2 + 1) \in \mathbb{F}_q[x]$. Then $g(0) = 0, g(1) = 2, g(2) = 2^{k-1}$, so $g(x)$ is a permutation polynomial of \mathbb{F}_q if and only if $2^{k-1} \equiv 1 \pmod{3}$, that is, k is odd. Hence f permutes \mathbb{F}_q if and only if k is odd.

(3) Let $q > 3$.

(3.1) The following proof is the same as that of Theorem 1.27. By

Proposition 1.14, f permutes \mathbb{F}_q if and only if $x^k - \alpha x^{k-2}$ permutes \mathbb{F}_q where $\alpha = -ba^{-1}$. Assume that f permutes \mathbb{F}_q . Suppose that $q \equiv \pm 1 \pmod{k}$ and $b \neq 0$. Then $\alpha \neq 0$. Let $n = \frac{q \pm 1}{k}$. Then $n \neq q - 1$. By Lemma 1.10 and the fact that f is a permutation polynomial of \mathbb{F}_q ,

$$\begin{aligned} 0 &= \sum_{w \in \mathbb{F}_q} (w^k - \alpha w^{k-2})^n \\ &= \sum_{w \in \mathbb{F}_q} \sum_{i=0}^n \binom{n}{i} (w^k)^{n-i} (-\alpha w^{k-2})^i \\ &= \sum_{w \in \mathbb{F}_q} \sum_{i=0}^n \binom{n}{i} (-\alpha)^i w^{kn - ki + ki - 2i} \\ &= \sum_{i=0}^n \binom{n}{i} (-\alpha)^i \sum_{w \in \mathbb{F}_q} w^{kn - 2i}. \end{aligned}$$

By Lemma 1.10, if $kn - 2i \neq q - 1$, then $\sum_{w \in \mathbb{F}_q} w^{kn - 2i} = 0$.

Assume that $kn - 2i = q - 1$. Either $kn = q - 1$ which implies $i = 0$

or $kn = q + 1$ which implies $i = 1$. Then either, when $kn = q - 1$, $0 = \sum_{i=0}^n \binom{n}{i} (-\alpha)^i \sum_{w \in \mathbb{F}_q} w^{kn-2i} = \sum_{w \in \mathbb{F}_q} w^{q-1} = -1$, a contradiction, or if $kn = q + 1$, then $0 = \sum_{i=0}^n \binom{n}{i} (-\alpha)^i \sum_{w \in \mathbb{F}_q} w^{kn-2i} = n(-\alpha) \sum_{w \in \mathbb{F}_q} w^{q-1}$, so $0 = \sum_{w \in \mathbb{F}_q} w^{q-1}$, a contradiction. Hence either $q \not\equiv \pm 1 \pmod{k}$ or $b = 0$.

(3.2) Assume that $x^2 + ba^{-1}$ has a root in \mathbb{F}_q . We have that

$$f \text{ permutes } \mathbb{F}_q \iff x^{k-2}(x^2 + ba^{-1}) \text{ permutes } \mathbb{F}_q.$$

By Theorem 1.13, (i) is trivial. To show that (ii) holds, assume that $b \neq 0$. Then $ba^{-1} \neq 0$, so the root of $x^2 + ba^{-1}$ is not zero.

If $k > 2$, then $x^{k-2}(x^2 + ba^{-1})$ has at least two distinct roots, so $x^{k-2}(x^2 + ba^{-1})$ is not a permutation polynomial of \mathbb{F}_q and so f is not a permutation polynomial of \mathbb{F}_q .

If $k = 2$, then

$$\begin{aligned} f \text{ permutes } \mathbb{F}_q &\iff x^2 + ba^{-1} \text{ permutes } \mathbb{F}_q \\ &\iff g.c.d.(2, q-1) = 1 \\ &\iff q \text{ is even} \\ &\iff \mathbb{F}_q \text{ has characteristic } 2. \end{aligned}$$

Hence (ii) holds. □

Theorem 1.28 was due to C.Small. Our next result gives an analysis of some larger classes.

Theorem 3.11. Let $f(x) = x^i - ax^j$, $i > j \geq 1$, $0 \neq a \in \mathbb{F}_q$, and put $k = i - j$.

Then

(1) For $i < q - 1$ and $k \geq 2$, if $i \mid (q - 1 + k)$ but $p \nmid \frac{q-1+k}{i}$, then $f(x)$ is not a permutation polynomial of \mathbb{F}_q .

(2) Assume that $(q - 1) \mid k$ and $(q - 1)$ does not divide i , $i - k$, $2i$, $2i - k$, $2i - 2k, \dots$, $(q - 2)i$, $(q - 2)i - k$, $(q - 2)i - 2k, \dots$, $(q - 2)i - (q - 2)k$. Then $a \neq 1$ if and only if $f(x)$ is a permutation polynomial of \mathbb{F}_q .

(3) If $(q - 1)$ does not divide $((q - 1)i - k), \dots, ((q - 1)i - (q - 2)k)$, then $f(x)$ is not a permutation polynomial of \mathbb{F}_q .

Proof. (1) Let $i < q - 1$ and $k \geq 2$. Since $2 \leq k < i < q - 1$, $q > 3$. Assume that $i \mid (q - 1 + k)$ and $p \nmid \frac{q-1+k}{i}$, say $ir = q - 1 + k$. If $r = 1$, then $i = q - 1 + k \geq q - 1$ which contradicts $i < q - 1$. Thus $r > 1$. Since $k(r - 1) = kr - k < ir - k = q - 1$, $r - 1 < \frac{q-1}{k} < \frac{q-1}{2}$, $r < \frac{q+1}{2} < q - 1$ (using $q > 3$). Thus $1 < r < q - 1$. Suppose that $f(x)$ is a permutation polynomial of \mathbb{F}_q . By Lemma 1.10,

$$0 = \sum_{w \in \mathbb{F}_q} (w^i - aw^j)^r = \sum_{t=0}^r \binom{r}{t} (-a)^t \sum_{w \in \mathbb{F}_q} w^{i(r-t)+jt}.$$

Since $i(r - t) + jt = ir - kt = q - 1 + (1 - t)k$, the w -exponents in the sum, for $t = 0, 1, \dots, r$, are $q - 1 + k$, $q - 1$, $q - 1 - k$, $q - 1 - 2k, \dots$, $q - 1 + (1 - r)k$. Since $k < i < q - 1$, and $0 \leq i(r - t) + jt = ir - kt \leq q - 1$ for all $t = 1, \dots, r$, by Lemma 1.10, $0 = \sum_{t=0}^r \binom{r}{t} (-a)^t \sum_{w \in \mathbb{F}_q} w^{i(r-t)+jt} = r(-a)(-1) = ra$, so $p \mid r$, a contradiction. Hence $f(x)$ is not a permutation polynomial of \mathbb{F}_q .

(2) Assume that $(q - 1) \mid k$ and $(q - 1)$ does not divide i , $i - k$, $2i$, $2i - k$, $2i - 2k, \dots$, $(q - 2)i$, $(q - 2)i - k$, $(q - 2)i - 2k, \dots$, $(q - 2)i - (q - 2)k$. By Lemma 1.10 we have that

$$f \text{ permutes } \mathbb{F}_q \iff \sum_{w \in \mathbb{F}_q} (w^i - aw^j)^t = \begin{cases} 0 & \text{for } t = 0, 1, \dots, q - 2, \\ -1 & \text{for } t = q - 1. \end{cases}$$

Consider

$$t = 0: \sum_{w \in \mathbb{F}_q} (w^i - aw^j)^t = \sum_{w \in \mathbb{F}_q} 1 = 0.$$

$$t = 1: \sum_{w \in \mathbb{F}_q} (w^i - aw^j)^t = \binom{1}{0} \sum_{w \in \mathbb{F}_q} w^i + \binom{1}{1} (-a) \sum_{w \in \mathbb{F}_q} w^{i-k} = 0.$$

$$\begin{aligned} t = 2: \sum_{w \in \mathbb{F}_q} (w^i - aw^j)^t &= \binom{2}{0} \sum_{w \in \mathbb{F}_q} w^{2i} + \binom{2}{1} (-a) \sum_{w \in \mathbb{F}_q} w^{2i-k} \\ &\quad + \binom{2}{2} (-a)^2 \sum_{w \in \mathbb{F}_q} w^{2i-2k} \\ &= 0. \end{aligned}$$

\vdots

$$\begin{aligned} t = q-2: \sum_{w \in \mathbb{F}_q} (w^i - aw^j)^t &= \binom{q-2}{0} \sum_{w \in \mathbb{F}_q} w^{(q-2)i} + \binom{q-2}{1} (-a) \sum_{w \in \mathbb{F}_q} w^{(q-2)i-k} \\ &\quad + \cdots + \binom{q-2}{q-2} (-a)^{q-2} \sum_{w \in \mathbb{F}_q} w^{(q-2)i-(q-2)k} \\ &= 0. \end{aligned}$$

$$\begin{aligned} t = q-1: \sum_{w \in \mathbb{F}_q} (w^i - aw^j)^t &= \binom{q-1}{0} \sum_{w \in \mathbb{F}_q} w^{(q-1)i} + \binom{q-1}{1} (-a) \sum_{w \in \mathbb{F}_q} w^{(q-1)i-k} \\ &\quad + \cdots + \binom{q-1}{q-1} (-a)^{q-1} \sum_{w \in \mathbb{F}_q} w^{(q-1)i-(q-1)k} \\ &= (-1)(1-a)^{q-1}. \end{aligned}$$

If $a = 1$, then $\sum_{w \in \mathbb{F}_q} (w^i - aw^j)^{q-1} = 0$, implying that $f(x)$ is not a permutation polynomial of \mathbb{F}_q .

If $a \neq 1$, then $\sum_{w \in \mathbb{F}_q} (w^i - aw^j)^{q-1} = -1$, so $f(x)$ is a permutation polynomial of \mathbb{F}_q .

(3) Assume that $(q-1) \nmid ((q-1)i-k), \dots, ((q-1)i-(q-2)k)$. From the proof of (2), $\sum_{w \in \mathbb{F}_q} (w^i - aw^j)^{q-1} = (-1) + (-a)^{q-1}(-1) = -2 \neq -1$, so $f(x)$ is not a permutation polynomial of \mathbb{F}_q . \square

Example 3.12. Let $f(x) = x^5 - 2x^3 \in \mathbb{F}_3[x]$. By Theorem 3.11(2), f is a permutation polynomial of \mathbb{F}_q .

Example 3.13. Let $f(x) = x^5 - x^3 \in \mathbb{F}_3[x]$. By Theorem 3.11(2), f is not a permutation polynomial of \mathbb{F}_q .

The next theorem is an extension of Proposition 1.29(2), which was due to C.Small.

Theorem 3.14. Let a be a primitive element in \mathbb{F}_q (i.e., a generator for the multiplicative group \mathbb{F}_q^*) where $q = p^n$ and $f(x) = x^{p^s} - ax^{p^r}$ where $s > r \geq 0$. Then f permutes \mathbb{F}_q if and only if one of the following conditions holds:

- (1) $p > 2$;
- (2) $p = 2$ and $\text{g.c.d.}(s - r, n) > 1$.

Proof. From Proposition 1.29(1), we have that f permutes \mathbb{F}_q if and only if a is not a $(p^s - p^r)^{\text{th}}$ power in \mathbb{F}_q .

We claim that a is not a k^{th} power in \mathbb{F}_q if and only if $\text{g.c.d.}(k, q - 1) = d > 1$.

Assume that $d = 1$. Then $uk + v(q - 1) = 1$ for some $u, v \in \mathbb{Z}$, so $uk - 1 = (q - 1)(-v)$. Thus $a^{uk-1} = a^{(q-1)(-v)} = 1$. Then $(a^u)^k = a^{uk} = a$. Since a is a primitive element, $a^u = w$ for some $w \in \mathbb{F}_q$. Hence $a = w^k$, a k^{th} power.

Assume that $a = w^k$ for some $w \in \mathbb{F}_q$. Since $0 \neq a$ is a primitive element, $w = a^u$ for some integer u , $1 \leq u \leq q - 1$. Then $a = a^{uk}$, and so $a^{uk-1} = 1$. Thus $uk - 1 = (q - 1)v$ for some $v \in \mathbb{Z}$. Since $d \mid k$ and $d \mid (q - 1)$, $d \mid 1$, so $d = 1$, and the claim is proved.

From this claim we deduce that

$$f \text{ permutes } \mathbb{F}_q \iff \text{g.c.d.}(p^s - p^r, q - 1) > 1.$$

Case 1. $p = 2$. Then

$$\begin{aligned}g.c.d.(p^s - p^r, q - 1) &= g.c.d.(2^s - 2^r, 2^n - 1) \\ &= g.c.d.(2^r(2^{s-r} - 1), 2^n - 1) \\ &= g.c.d.(2^{s-r} - 1, 2^n - 1) \\ &= 2^{g.c.d.(s-r, n)} - 1.\end{aligned}$$

Thus $g.c.d.(p^s - p^r, q - 1) = 1$ if and only if $g.c.d.(s - r, n) = 1$.

Case 2. $p \neq 2$. Then

$$\begin{aligned}g.c.d.(p^s - p^r, q - 1) &= g.c.d.(p^r(p^{s-r} - 1), p^n - 1) \\ &= g.c.d.(p^{s-r} - 1, p^n - 1).\end{aligned}$$

Since $p \neq 2$, $s - r \geq 1$ and $n \geq 1$, $2 \mid g.c.d.(p^{s-r} - 1, p^n - 1)$, so $g.c.d.(p^s - p^r, q - 1) \geq 2 > 1$.

Hence f permutes \mathbb{F}_q if and only if (1) or (2) holds. □

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

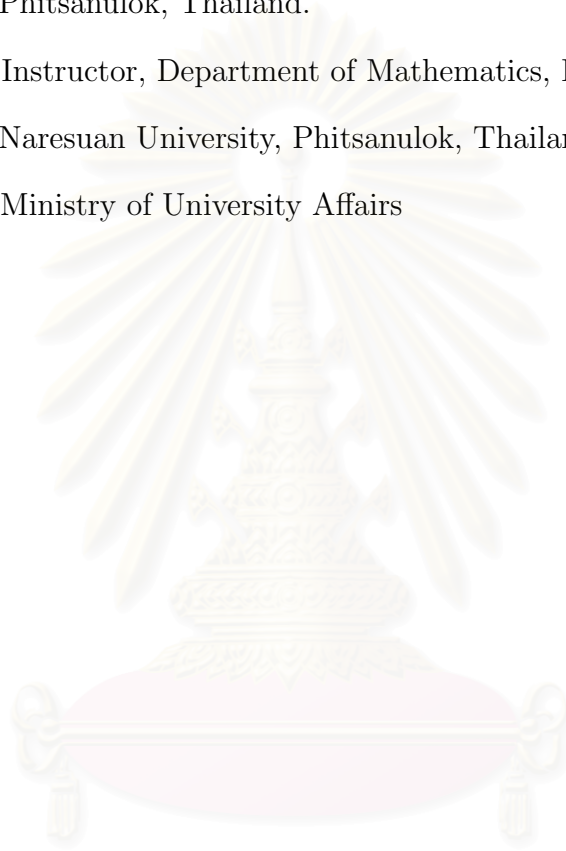
REFERENCES

1. Dickson, L.E. Linear Groups with an Exposition of the Galois Field Theory.
New York: Dover, 1958.
2. Dickson, L.E. The Analytic Representation of Substitutions. Ann. of Math.
11(1896-97): 65 - 120.
3. Lidl, R. & Mullen, G.L. When does a Polynomial over a Finite Field permute
the Elements of the Field ?. Amer. Math. Monthly 95(1988): 243 - 246.
4. Lidl, R. & Mullen, G.L. When does a Polynomial over a Finite Field permute
the Elements of the Field ?, II. Amer. Math. Monthly 100(1993): 71 - 74.
5. Lidl, R. & Niederreiter, H. Finite Fields. Addison-Wesley, 1983.
6. Mollin, R.A. & Small, C. On Permutation Polynomials over Finite Fields.
Internat. J. Math. and Math. Sci. 10(1987): 535 - 544.
7. Small, C. Permutation Binomials. Internat. J. Math. and Math. Sci. 13(1990):
337 - 342.
8. Small, C. Arithmetic of Finite Fields. New York: Marcel Dekker, 1991.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

VITA

- Name** : Miss Suphawan Janphaisaeng
- Degree** : Bachelor of Science (Mathematics), 1996, Naresuan University,
Phitsanulok, Thailand.
- Position** : Instructor, Department of Mathematics, Faculty of Science,
Naresuan University, Phitsanulok, Thailand.
- Scholarship** : Ministry of University Affairs



สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย