CLASSES OF PERMUTATION POLYNOMIALS OF THE TYPE $(X^P - X + \delta)^S + X$ OVER FINITE FIELDS

BY

GAURAV CHAUHAN

SUPERVISED BY

Dr.SOUMEN MAITY

THESIS SUBMITTED TOWARDS PARTIAL FULFILLMENT

OF

BS-MS DUAL DEGREE

AT

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH

PUNE, INDIA

APRIL 11,2011

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH

DEPARTMENT OF MATHEMATICS

The undersigned hereby certify that they have read and recommend to the Faculty of UNDERGRADUATE STUDIES for acceptance a thesis entitled "CLASSES OF PERMUTATION POLYNOMIALS OF THE TYPE $(x^p - x + \delta)^s + x$ OVER FINITE FIELDS" which represents original research carried out by GAURAV CHAUHAN under the supervision of Dr.SOUMEN MAITY in partial fulfillment of the requirements for the degree of BS-MS DUAL DEGREE.

Dated: April 11,2011

Supervisor: _____

Dr.SOUMEN MAITY

Head (Mathematics): _____

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH

Date: **April 11,2011**

Author: GAURAV CHAUHAN

Title: CLASSES OF PERMUTATION POLYNOMIALS OF THE TYPE $(x^p - x + \delta)^s + x$ OVER FINITE FIELDS

Department: MATHEMATICS

Degree: BS-MS Convocation: **May 8** Year: **2011**

Signature of Author

To IISER Pune

Table of Contents

Abstract

Permutation polynomials have for long been an area of immense interest for researchers worldwide. Though properties of permutation polynomials have been well documented, few special classes of permutation polynomials are presently known.
Recent application of permutation polynomials in construction of public key encryption protocols has provided major incentive towards research in this area. A major direction of current research is construction of some special classes.

The aim of this work is to study latest research in this area and building upon the techniques therein provide some new classes of permutation polynomials over finite fields. Most of the work done is inspired by research of Cunsheng Ding et al [5, 6]. The research utilizes their method of obtaining the permutation polynomials using computations and explaining their class by theoretical methods.

The particular kind of polynomials studied are $(x^p - x + \delta)^s + x$ *over the field* $\mathbb{F}_{p^m}$ *for different values of s.*
Besides a synopsis of results published recently, main results of this thesis are essentially contained in various chapters dealing with polynomials over separate fields based upon the base prime number. Some of the new classes formed thereby are not particular to those fields and could be immensely useful for general applications.

Acknowledgements

At the very onset, I would like to extend my gratitude towards each and everyone who has been a help in this project from inception to its culmination.
I would like to thank Dr.Soumen Maity, Assistant Professor,Department of Mathematics,IISER Pune who is my thesis supervisor for his many suggestions and continous support during this research.

At the same time I am also grateful to other faculty members and staff at my alma mater IISER Pune.In particular, I must thank Dr.Anupam Singh,my faculty coordiantor.

It was pioneering work by Prof. Tor Helleseth (University of Bergen) and Prof.Victor Ginoviev (Russian Academy of Sciences) in the area of permutation polynomials which have inspired subsequent research in this area, including mine. As such it is obligatory I must express my regards for them. Immediate inspiration, for which I am grateful, to pick up this problem comes from recent research conducted by Prof.Cunsheng Ding, Hong Kong University of Science and Technology and Jin Yuan, Macquarie University,Australia.

Goes without mention, I can't be more grateful to my parents, family and friends for their patience and support. Without them this work would never have come into existence (literally).
Finally, I wish to thank the following: Hall of Residence 1 students (for making my days less boring); Mr.Tim Burners-Lee, Director www Consortium (for illuminating me) and friends who kept me from going to HRI, Allahabad for final year project and the Almighty(whom I encountered many times since January,2011).

Preface

This thesis contains work on permutation polynomials over finite fields.Besides a survey of published and basic results in this area, there are also contained a few original results on the classes of permutation polynomials over finite fields.

Chapter 1 contains a collection of all the basic results of permutation polynomials from standard text, those which shall be used in subsequent chapters in proving various classes of polynomials to be permutations. The results are motivated by the study of [4] and [3].

Chapter 2 is a reproduction of results obtained in the research of Cunsheng Ding and Jin Yuan [5], [6]. It contains classes of polynomials over finite fields of even cardinality based on the relation of Kloosterman identities and permutation polynomials.

Results in chapter 3 and 4 are classes of permutation polynomials over finite fields of odd cardinality, an extension work inspired by the results of chapter 2.

Throughout the thesis, extensive use of MATLAB computing has been made. In view of recent applications of permutation polynomials in Turbo codes and LDPC codes, this work becomes even more interesting.

Chapter 1

Permutation Polynomials: An Introduction

1.1 Permutation Polynomials

This thesis is a summary of classes of permutation polynomials obtained as a result of recent research inspired by the investigation of relation between Kloosterman sums and special type of polynomials discussed in this thesis throughout. This kind of work was pioneered by Helleseth and Zinoviev [2].

This chapter develops the notion of permutation polynomial over a finite field and provides results which shall be used subsequently in different chapters to construct new classes of permutation polynomials. We shall start by defining a permutation polynomial over a finite field.

Definition 1.1.1. *Let $\mathbb{F}_{p^m}$, where p is a prime, be a finite field. Then a polynomial $f(x) \in \mathbb{F}_{p^m}[x]$ is called a permutation polynomial if the associated function $f : c \to f(c)$ is a permutation of $\mathbb{F}_{p^m}$.*

The existence of permutation polynomials is trivial as every mapping of a finite

field into itself is expressible as a polynomial. Linear transformations are also an example of permutation polynomial.

There are however a few more profound problems associated with these polynomials. Determination of a permutation polynomial is a long settled question, which following section shall answer, but for arbitrary polynomials to be permutations, conditions are normally complicated and of larger interest.

1.2 Criteria for permutation polynomials

If we have a polynomial $f(x)$ over a finite field $\mathbb{F}_{p^m}$, the question one may ask is:

How do we determine if the polynomial is a permutation polynomial for the finite field?

The answer, thanks to the finiteness of the field, is quite easy to provide.

Lemma 1.2.1. *The polynomial $f(x) \in \mathbb{F}_{p^m}$ is a permutation polynomial over $\mathbb{F}_{p^m}$ if and only if one of these conditions is satisfied:*

1. *the function $f : c \rightarrow f(c)$ is onto*
2. *the function $f : c \rightarrow f(c)$ is one-one*
3. *f(x) = d has one solution in $\mathbb{F}_{p^m}$ for all d*
4. *f(x) = d has a unique solution in $\mathbb{F}_{p^m}$ for all d*

Although, all the above conditions are equivalent, the one most used in practice and which shall repeatedly be invoked in this thesis is the last one. Clearly, if a finite field is permuted by a function, the function has to be one-one and onto.
Many other criterion could be provided for the polynomials to be permutation, but we shall restrain with the following important one.

1.3 Hermite's criterion and consequences

Theorem 1.3.1. *(Hermite's criterion):Let $\mathbb{F}_{p^m}$ be a finite field. Then $f \in \mathbb{F}_{p^m}[x]$ is a permutation polynomial over it if and only if following two conditions hold:*

1. *f has exactly one root in $\mathbb{F}_{p^m}$*
2. *for each integer t with $1 \leq t \leq p^m - 2$ and t not divisible by p, the residue $f(x)^t mod(x^{p^m} - x)$ has degree $\leq p^m - 2$*

A detailed proof for the theorem is given in [3]. Above theorem is a widely used criterion for establishing a polynomial to be a permutation polynomial. One of its major corollaries is given below.

Corollary 1.3.2. *If $d > 1$ is a divisor of $p^m - 1$ then there is no permutation polynomial of degree d over $\mathbb{F}_{p^m}$.*

Proof. If $deg(f) = d$, then $deg(f^{(p^m-1)/d})$ is $p^m - 1$. Hence the last condition of Hermite's criterion is violated. □

Precisely for above reason, if $f(x)$ is a permutation polynomial, then $f(x)^k$ is a permutation polynomial if and only if k is coprime to $p^m - 1$.
Due to this, in subsequent chapters, whenever a polynomial is raised to some power, care is taken to ascertain that the exponent is relatively coprime to $p^m - 1$, in order not to change the permutation nature of the given polynomial.
In most cases, we have made use of the prime integer p itself. Details can be seen in further sections.

In the next section we shall discuss some basic types of permutation polynomials which are encountered more often. In later chapters, we shall try and recognize these basic classes before going for more complex ones.

1.4 Elementary permutation polynomials

In this section various examples of simplest forms of permutation polynomials are discussed. Often, complicated classes of permutation polynomials can be reduced to one of these general classes by certain manipulations, thereby proving their permutation nature.

Theorem 1.4.1.

1. *Every linear polynomial over $\mathbb{F}_{p^m}$ is a permutation polynomial*
2. *The monomial x^n is a permutation polynomial over $\mathbb{F}_{p^m}$ if and only if $(n, p^m - 1) = 1$.*

Proof. Part (1) is trivial, as linear polynomials are one-one. Part(2) is consequence of the property that in a finite field, the function $f : \ c \rightarrow c^n$ is onto if and only if $(n, p^m - 1)$ is 1. □

1.4.1 Linearized polynomials

Definition 1.4.1. *Polynomials of the type* $L(x) = \sum_{i=0}^{m} a_i x^{p^i}$ *with* $a_i \in \mathbb{F}_p$ *is called a linearized polynomial over* $\mathbb{F}_{p^m}$.

We now see when can a linearized polynomial be a permutation.

Theorem 1.4.2. *A linearized polynomial L(x) is a permutation polynomial if and only if it has no non-zero root in the field* $\mathbb{F}_{p^m}$.

Proof. $L(x)$ is a linear operator over $\mathbb{F}_{p^m}$ taken as a vector space over base field. A linear operator can only be one-one if $ker(L)$ is zero. This implies that only root of the polynomial is 0. □

A lot of polynomials that we shall see in subsequent chapters fall under this class of permutation polynomials. This is by far one of the most common type of permutations.
From here we move to another special type of polynomials which have been studied extensively[4].

1.4.2 Dickson's Polynomials

We shall now discuss a new class of polynomials called *Dickson's polynomials* which give some new classes of permutation polynomials.

Definition 1.4.2. *The polynomial of the type*
$g_k(x,a) = \sum_{j=0}^{\lfloor (k/2) \rfloor} \frac{k}{k-j}\binom{k-j}{j}(-a)^j x^{k-2j}$ *is called a Dickson's polynomial of degree* k *over* $\mathbb{F}_{p^m}$.

Similar to above case, Dickson's polynomials are permutation polynomials under certain conditions.

Theorem 1.4.3. *The Dickson's polynomial* $g_k(x,a)$ *is a permutation polynomial if and only if* $gcd(k, p^{2m} - 1)$.

For results on Dickson's polynomials the reader is referred to [4]. In subsequent chapters, arbitrary polynomials are manipulated to convert them to appropriate Dickson's polynomials and hence establish that they are permutation polynomials.

We have now mentioned all the basic permutation polynomials that we need to use in further chapters of this thesis. The type of permutation polynomials we are about to deal with are:
$(x^p - x + \delta)^s + x$ where δ is an element of $\mathbb{F}_{p^m}$ with non-zero trace and s is an integer.
There are reasons to choose this particular type which are discussed in next section.

1.5 Kloosterman polynomials

We start by defining weight of an integer c.

Definition 1.5.1. *Let the binary representation of an integer* $c = \sum c_i 2^i$. *Then the weight is defined as* $w(c) = \sum c_i$.

Given integers $c, d \in (0, 1, ..., 2^m - 1)$ we define a polynomial function as follows:

$$L_{c,d}(x) = \sum c_i x^{2^i} + \sum \frac{d_i}{x^{2^i}}$$

given that $L_{c,d}(0) = 0$.

Definition 1.5.2. *Let* $e = w(c)$ *mod 2. The polynomial* $L_{c,d}(x)$ *on* $\mathbb{F}_{2^m}$ *is called a Kloosterman polynomial if* $w(d)$ *is even and* $L_{c,d}$ *maps the set of trace 1 elements bijectively to trace* e *elements.*

The objective of this section is to present a relationship between Kloosterman polynomials and the permutation polynomials of a special form. Ding and Yuan [6] have shown that $L_{1,d} = x + \sum \frac{d_i}{x^{2^i}}$ is a Kloosterman polynomial if and only if for some $\delta \in \mathbb{F}_{2^m}, Trace(\delta) = 1$ the polynomial $\frac{1}{L_d(x) + \delta} + x$ is a permutation polynomial.

This motivated research to find such permutation polynomials in case of $d = 10$ and subsequent chapters deal with the classes of permutation polynomials obtained as a result of that enquiry.

A very special type of permutation polynomial were obtained as a result in identifying new Kloosterman identities and these are the type of polynomials we shall focus upon.

1.6 Conclusion

In Helleseth and Zinoviev [2], some new identities for Kloosterman sums were introduced. The subsequent research in this thesis is motivated by findings that the polynomials of the type, $(x^p - x + \delta)^s + x$ are permutation polynomials over $\mathbb{F}_{2^m}$ for some values of s.

Extending the idea to finite fields of odd cardinality, we found that similar results are obtained there too. It is however a difficult task to show how such polynomial forms arise.

Nevertheless, it is a helpful technique to search for various new classes of permutation polynomials. This chapter contains a summary of important results about permutation polynomials over finite fields. For a detailed study reader is advised to refer to [3].

Chapter 2

Permutation Polynomials over $\mathbb{F}_{2^m}$

2.1 Introduction

Permutation polynomials associated with Kloosterman sum identities have brought about a new method to construct classes. Helleseth and Zinoviev [2] made use of permutation polynomials of following kind in determining new Kloosterman sum identities over $\mathbb{F}_{2^m}$:
$(x^2 - x + \delta)^s + x = (x^2 + x + \delta)^s + x$ for δ an element of $\mathbb{F}_{2^m}$ with non zero trace.

While the explanation for only 2 classes was provided in [2], some other classes were explained by Cunsheng Ding et al [5]. The method employed is repeated in all other chapters. Using a computer program, values of s for which the above polynomial is a permutation of $\mathbb{F}_{2^m}$ are obtained. Theoretical explanations are subsequently provided for those polynomials in form of classes of permutation polynomials.

Our interest is in the values s such that $2 \leq s \leq 2^m - 2$ and $(x^2 + x + \delta)^s + x$ is a permutation polynomial for δ an element of $\mathbb{F}_{2^m}$ with non-zero trace. For $s = 1$ the

polynomial reduces to a monomial x^2 which is a permutation polynomial by Theorem 1.4.1(ii). These values are numerated in the table 2.1 given in the section 2.2.
This chapter contains four special classes of permutation polynomials over $\mathbb{F}_{2^m}$. Some of the values are as yet not classified but an attempt to a possible solution has been provided.

2.2 Computed values of s for different m

Following the methods of Helleseth and Zinoviev [2], using a MATLAB program, designed for calculations over general finite fields of even cardinality, following values of s were obtained such that $(x^2 + x + \delta)^s + x$ is a permutation polynomial over $\mathbb{F}_{2^m}$. The values of interest are of course those lying in between 2 and $2^m - 2$.

Table 2.1: Values of s for which $(x^2 - x + \delta)^s + x$ permutes $\mathbb{F}_{2^m}$

m	*minimal polynomial*	δ	s
5	$x^5 + x^2 + 1$	α^5	2^a , 4^a , 8^a , 14 , 16^a , 21^c , 29^b , 30^b
6	$x^6 + x + 1$	α^5	4^a, 5, 8^a, 28^d, 32^a, 61^b, 62^b
7	$x^7 + x + 1$	α^7	2^a, 8^a, 32^a, 64^a, 85^c, 125^b, 126^b
8	$x^8 + x^5 + x^3 + x + 1$	α^3	2^a, 4^a, 8^a, 16^a, 32^a, 64^a, 120^d, 128^a, 165^e, 253^b, 254^b

In the table each value has been marked with a letter which indicates the class of permutation polynomial it corresponds to. The description of all classes is provided in the rest of the chapter.

2.3 Linearized permutation polynomials

We have seen in previous chapter that one of the most commonly found class of the permutation polynomials is that of linearized polynomials. We shall identify these from the table first.

Let $s = 2^k$ for some integer k. Then the polynomial reduces to:

$(x^2 + x + \delta)^{2^k} + x = (x^{2^{k+1}} + x^{2^k} + \delta^{2^k}) + x$

Above polynomial is the sum of a linearized polynomial $L(x) = (x^{2^{k+1}} + x^{2^k} + x)$ and a constant.

Values marked with a in the table correspond to this class. Using a computer program it can be ascertained that these values satisfy the conditions of theorem1.4.2.Hence they are permutation polynomials.

Other values of s missing from the table which are powers of 2 don't satisfy this condition.

2.4 Polynomials with $s = (2^m - i)$: $i = 2, 3$.

For each value of m there are certain values of s marked with b. These values were shown by Helleseth and Zinoviev [2] to be corresponding to a new class of permutation polynomials. In this section we shall discuss that result and reproduce it in a compact way.

The values marked b correspond to $s = 2^m - 2$ or $s = 2^m - 3$. Given below is the lemma which shall provide the classification of such polynomials.

Lemma 2.4.1. *Let $\delta \in \mathbb{F}_{2^m}$ be an element with Trace 1. Then in each of the cases*

$i = 2, 3$ $p(x) = (x^2 + x + \delta)^{2^m-i} + x$ *is a permutation polynomial.*

Proof. First we consider the case when $i = 2$. Then we show that $p(x) = a$ has a unique solution in $\mathbb{F}_{2^m}$. Since $Tr(\delta) = 1$, $(x^2 + x + \delta) \neq 0$ for all x. Then suppose $p(x) = a$

$$(x^2 + x + \delta)^{2^m-2} + x = a \tag{2.4.1}$$

$$\frac{1}{(x^2 + x + \delta)} + x = a \tag{2.4.2}$$

$$1 + x((x^2 + x + \delta)) = a(x^2 + x + \delta) \tag{2.4.3}$$

$$x^3 + (a+1)x^2 + (a+\delta)x + a\delta + 1 = 0 \tag{2.4.4}$$

Replacing x by $y + a$ we have

$$y^3 + ax^2 + a^2x + ax^2 + a^2 + ax + \delta x + a^2 + 1 = 0 \tag{2.4.5}$$

$$y^3 + y^2 + (a^2 + a + \delta)y + 1 = 0. \tag{2.4.6}$$

Let $b = (a^2 + a + \delta)$, then $Tr(b) = Tr(\delta) = 1$. Replacing $y = z + 1$, we have

$$z^3 + (b + 1)z + b + 1 = 0, \;\; Tr(b) = 1 \tag{2.4.7}$$

We need to show that above equation has atmost one solution in $\mathbb{F}_{2^m}$. It is known from Berlekemp et al that this is possible if $Tr(b + 1) \neq Tr(1)$ which is evidently true.

For the second part, we assume there are two solutions to the equation $p(x) = a$

$x, y \in \mathbb{F}_{2^m}$. Then,

$$(x^2 + x + \delta)^{2^m-3} + x = (y^2 + y + \delta)^{2^m-3} + y \tag{2.4.8}$$

$$\frac{1}{(x^2 + x + \delta)^2} + x = \frac{1}{(y^2 + y + \delta)^2} + y \tag{2.4.9}$$

Transferring and multiplying by denominators we have

$$\begin{aligned}(x + y)(((x^2 + x + \delta)(y^2 + y + \delta))^2 \\ = (x^2 + x + \delta + y^2 + y + \delta)^2 \\ (x + y)((x^2 + x)(y^2 + y) + \delta(x^2 + x + y^2 + y) + \delta^2)^2 \\ = (x^2 + y^2 + x + y)^2\end{aligned}$$

Substituting $u = (x + y)$ and $v = xy$, we have following equation.

$$u(v(u + v + 1) + \delta(u^2 + u) + \delta^2)^2 = (u^2 + u)^2 \tag{2.4.10}$$

Raising both sides by 2^{m-1} we have

$$v^2 + (u+1)v + \delta(u^2+u) + \delta^2 + (u^2+u)/u^{2^{m-1}} = 0 \tag{2.4.11}$$

Now if, $u = 1$,$v = \delta$, then $Tr(v/u^2) = 1$. This means that the polynomial $(z^2 + uz + v)$ has no solution in $\mathbb{F}_{2^m}$. This is a contradiction since x, y are assumed to be two roots of this polynomial. So, $u \neq 1$.

Assume $u \neq 0$. Then, the equation 2.4.11 has a solution for v only if following is true

$$Tr(\frac{\delta(u^2+u) + \delta^2 + (u^2+u)/u^{2^{m-1}}}{(u+1)^2}) = 0 \tag{2.4.12}$$

However, we have by trace calculations,

$$\begin{aligned} Tr(\frac{\delta(u^2+u) \ + \ \delta^2 \ + \ (u^2+u)/u^{2^{m-1}}}{(u+1)^2}) &= Tr(\frac{\delta u}{u+1} \ + \ \frac{\delta}{u+1} \ + \ \frac{u}{(u+1)u^{2^{m-1}}}) \\ &= Tr(\delta \ + \ \frac{u^2}{(u+1)^2 u}) \\ &= 1 \ + \ Tr(\frac{u^2}{(u+1)^2 u}) \\ &= 1 \ + \ Tr(\frac{1}{u+1} \ + \ \frac{1}{(u+1)^2}) \\ &= 1 \end{aligned}$$

Hence, $u \ = \ 0$. So, $x \ = \ y$. This ends the proof. □

We shall now proceed towards the next section of the chapter.

2.5 Polynomials when m is odd

Suppose m is an odd integer. Then we can provide a class, due to [5] of permutation polynomials. Let k and m be two positive integers. We know $2^k + 1$ and $2^m - 1$ are coprime if and only if $\frac{m}{gcd(k,m)}$ is odd [1].

Theorem 2.5.1. *Let δ be trace 1 element of $\mathbb{F}_{2^m}$ and let $\frac{m}{gcd(k,m)}$ be an odd number. Then $f(x) = (x^{2^k} \ + \ x \ + \ \delta)^{k'} \ + \ x$ is a permutation polynomial whenever $k'(2^k + 1) \ \equiv \ 1 \ mod \ (2^m \ - \ 1)$.*

Proof. $2^k + 1$ and $2^m - 1$ are coprime. Then raising the power to $(2^k + 1)$ on both sides of the following equation:

$$(x^{2^k} + x + \delta)^{k'(2^k+1)} = (c+x)^{2^k+1},\ c \in \mathbb{F}_{2^m}$$
$$(x^{2^k} + x + \delta) = (c+x)^{2^k+1}$$

It suffices to show that above equation does not have more than one solutions. Reformulating the equations as follows:

$$x^{2^k} + x + \delta + x^{2^k+1} + cx^{2^k} + c^{2^k}x + c^{2^k+1} = 0 \quad (2.5.1)$$
$$x^{2^k+1} + (c+1)x^{2^k} + (c+1)^{2^k}x + c^{2^k+1} + \delta = 0 \quad (2.5.2)$$
$$(x+c+1)^{2^k+1} + (c^{2^k+1} + c^{2^k} + c + 1 + \delta) = 0 \quad (2.5.3)$$
$$(x + c + 1)^{2^k+1} = d \quad (2.5.4)$$

Since $(2^k + 1)$ is coprime to $(2^m - 1)$,then above equation is a permutation polynomial. Hence it has a unique solution. This completes the proof. □

For values of s marked as c polynomials correspond to the polynomials of above class with $k = 1$. Hence those values are explained by this class.

2.6 Polynomials when m is even

In case m is an even integer, this section discusses 3 classes of permutation polynomials on $\mathbb{F}_{2^m}$. Two of these are of the type studied in [2] and one is different. We shall start by following theorem due to [5].

Theorem 2.6.1. *For an even integer m and trace 1 element δ the polynomial $(x^2 + x + \delta)^s + x^{2^{m/2+1}}$ where $s = 2^{m/2} - 1$ is a permutation polynomial over $\mathbb{F}_{2^m}$.*

Proof. It suffices to show that the equation:

$$(x^2 + x + \delta)^{2^{m/2}-1} = (x^{2^{m/2+1}} + d) \tag{2.6.1}$$

has a unique solution for $d \in \mathbb{F}_{2^m}$.

Substituting $x^{2^{m/2}} = z$ we have:

$$z^2 + z + \delta^{2^{m/2}} = (z^2 + d)(x^2 + x + \delta) \tag{2.6.2}$$

Raising both sides by $2^{m/2}$, we get

$$(x^2 + x + \delta) = (x^2 + d^{2^{m/2}})(z^2 + z + \delta^{2^{m/2}}) \tag{2.6.3}$$

Multiplying 2.6.2 and 2.6.3 we have

$$(z^2 + d)(x^2 + d^{2^{m/2}}) = 1 \tag{2.6.4}$$

From 2.6.3 and 2.6.4

$$z^2 + z + \delta^{2^{m/2}} = \frac{(x^2 + x + \delta)}{(x^2 + d^{2^{m/2}})} \tag{2.6.5}$$

$$z = \frac{(x^2 + x + \delta + 1)}{(x^2 + d^{2^{m/2}})} + \delta^{2^{m/2}} + d \tag{2.6.6}$$

$$\frac{d(x^2 + d^{2^{m/2}}) + 1}{x^2 + d^{2^{m/2}}} = [\frac{(x^2 + x + \delta + 1) + (x^2 + d^{2^{m/2}})(\delta^{2^{m/2}} + d)}{(x^2 + d^{2^{m/2}})}]^2 \tag{2.6.7}$$

Taking all the powers of x together we obtain

$$x^4 = \frac{\delta^2 + 1 + \delta^{2^{m/2+1}} d^{2^{m/2+1}} + d^2 d^{2^{m/2+1}} + d d^{2^{m/2+1}} + \delta^{2^{m/2}}}{1 + \delta^{2^{m/2+1}} + d^2 + d} \tag{2.6.8}$$

Now $Tr(1 + \delta^{2^{m/2+1}} + d^2 + d) = Tr(\delta) = 1$ because $Tr(1) = 0$ as m is even.

Hence, $(1 + \delta^{2^{m/2+1}} + d^2 + d) \neq 0$ and x^4 is properly defined. Since monomial x^4 is a permutation polynomial, we have unique solution for x. This completes the proof of the theorem.

The values of s marked with d correspond to polynomials of this class. The corollary of this polynomial provides a different class altogether which is not similar to one discussed in [2]. □

We shall now detail another class of polynomials as a corollary to above theorem.

Corollary 2.6.2. *If m is even and δ is a trace one element of $\mathbb{F}_{2^m}$, then $(1 + \delta^2 + x^{2^{m/2}} + \delta^{2^{m/2+1}} x^{2^{m/2+1}} + x^{2^{m/2+1}+1} + x^{2^{m/2+1}+2})(1 + \delta^{2^{m/2+1}} + x + x^2)^{2^m-2}$ is a permutation polynomial of $\mathbb{F}_{2^m}$.*

Proof. From theorem2.6.1 we have

$$x^4 = \frac{\delta^2 + 1 + \delta^{2^{m/2+1}} d^{2^{m/2+1}} + d^2 d^{2^{m/2+1}} + d d^{2^{m/2+1}} + \delta^{2^{m/2}}}{1 + \delta^{2^{m/2+1}} + d^2 + d} = g(d) \tag{2.6.9}$$

We shall show that g is an injective map from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$. Suppose for $d_1, d_2 \in \mathbb{F}_{2^m}$, we have $g(d_1) = g(d_2)$. Since we have unique values of x for each d,hence let $f(x_i) = d_i$. So $x_1^4 = x_2^4$ implying that $x_1 = x_2$ as x^4 is a permutation polynomial. This means $d_1 = d_2$. Hence the map is injective. Since the injective mapping is on same fields hence it has to be a permutation. This completes the proof. □

This is a polynomial of different structure than the one we are dealing with. Obviously, there are no values of s which correspond to this class of polynomial in the table. We shall now describe another class of polynomials which is similar to the ones we are discussing in the thesis. This polynomial class is in the case when m is divisible by 4.

Theorem 2.6.3. *Let m be divisible by 4 and δ be an element with trace 1 in $\mathbb{F}_{2^m}$. Then $h(x) = (x^2 + x + \delta)^{(2^{m+1}-2^{m/2}-1)/3} + x$ is a permutation polynomial over $\mathbb{F}_{2^m}$.*

Proof. It suffices to show that $h(x) = d$ has a unique solution for all $d \in \mathbb{F}_{2^m}$. Since m is divisible by 4 hence $m/2 + 1$ and m are coprime. Then $2^{m/2+1} - 1$ and $2^m - 1$ are also coprime [1].
Consider the expression $\frac{(2^{m+1}-2^{m/2}-1)(2^{m/2+1}-1)}{3}$. We now have

$$\frac{(2^{m+1} - 2^{m/2} - 1)(2^{m/2+1} - 1)}{3} - (2^{m/2} - 1) \tag{2.6.10}$$

$$= \frac{(2^{m+1} - 2^{m/2} - 1)(2^{m/2+1} - 1) - 3(2^{m/2} - 1)}{3} \tag{2.6.11}$$

$$= \frac{2^{3m/2+2} - 2^{m+1} - 2^{m/2+1} - 2^{m+1} + 2^{m/2} - 2^{m/2+1} - 2^{m/2} + 4}{3} \tag{2.6.12}$$

$$= \frac{2^{3m/2+2} - 2^{m+2} - 2^{m/2+2} + 4}{3} \tag{2.6.13}$$

$$= \frac{4(2^{m/2} - 1)}{3}(2^m - 1) \tag{2.6.14}$$

Since m is even hence 3 divides $(2^{m/2} - 1)$. Therefore

$$\frac{(2^{m+1} - 2^{m/2} - 1)(2^{m/2+1} - 1)}{3} - (2^{m/2} - 1) = 0 mod (2^m - 1)$$

$\frac{(2^{m+1}-2^{m/2}-1)(2^{m/2+1}-1)}{3} = (2^{m/2}-1)\ mod(2^m-1)$.

Now raising both sides of the equation $h(x) = d$ by $(2^{m/2+1}-1)$ we have following equivalent equation.

$$(x^2+x+\delta)^{2^{m/2}-1} \ = \ (x+d)^{2^{m/2+1}-1} \tag{2.6.15}$$

Since $Tr(\delta) = 1$, hence $d \ \neq \ x$. Substituting $z = x^{2^{m/2}}$,we have following equations

$$(z^2+z+\delta^{2^{m/2}})(x+d) \ = \ (z^2+d^{2^{m/2}+1})(x^2+x+\delta) \tag{2.6.16}$$

Raising the power by $2^{m/2}$ on both sides, we get

$$(z+d^{2^{m/2}})(x^2+x+\delta) \ = \ (z^2+z+\delta^{2^{m/2}})(x^2+d^2) \tag{2.6.17}$$

Multiplying 2.6.16 and 2.6.17,

$$(x+d)(z+d^{2^{m/2}}) \ = \ 1 \tag{2.6.18}$$

$$z \ = \ \frac{1}{x+d} \ + \ d^{2^{m/2}} \tag{2.6.19}$$

Combining this result with2.6.16 we get,

$$z^2+\frac{1}{x+d}+d^{2^{m/2}}+\delta^{2^{m/2}} \ = \ \frac{(x^2+x+\delta)}{x^2+d^2}\frac{1}{(x+d)^3} \tag{2.6.20}$$

Transferring terms to right hand side, we have

$$z^2 \ = \ \frac{x+\delta+d^2+(d^{2^{m/2}}+\delta^{2^{m/2}})(x+d)^3}{(x+d)^3} \tag{2.6.21}$$

Combining 2.6.21 with the value of z obtained above, we get

$$\frac{x+\delta+d^2+(d^{2^{m/2}}+\delta^{2^{m/2}})(x+d)^3}{(x+d)^3} \ = \ \frac{(d^{2^{m/2}}x+d^{2^{m/2}}d+1)^2}{(x+d)^2} \tag{2.6.22}$$

Above equation is equivalent to following

$$(d^{2^{m/2}} + d^{2^{m/2+1}} + \delta^{2^{m/2}})(x+d)^3 \;=\; (d^2 + d + \delta) \tag{2.6.23}$$

Putting $z \;=\; (x+d)$ the equation obtained is

$$y^3 \;=\; (d^{2^{m/2}} + d^{2^{m/2+1}} + \delta^{2^{m/2}})^{2^{m/2}-1} \tag{2.6.24}$$

Since 3 divides $2^{m/2}-1$ the possible solutions of this equation are $(d^{2^{m/2}} + d^{2^{m/2+1}} + \delta^{2^{m/2}})^{(2^{m/2}-1)/3}\omega^i$ where ω is a cube root of unity and $i = \; 0, 1, 2$.

Assume that there are two possible solutions $y_i$and y_j. But we know that $y.y^{2^{m/2}} \;=\; 1$. Hence, $y_i^{2^{m/2}+1} \;=\; y_j^{2^{m/2}+1} = 1$. This implies that $\omega^{2^{m/2}+1} \;=\; 1$.

This however is not possible as $2^{m/2}+1$ is not divisible by 3. Hence, there can atmost be one y_i satisfying the condition. This argument completes the proof. □

In the table the values marked by e correspond to this class of permutation polynomial.

2.7 Conclusion

This chapter presented some classes of permutation polynomial over $\mathbb{F}_{2^m}$. However it is observed that there are 2 pairs of (m, s) values which do not correspond to any of the classes described above. They are $(5, 14)$ and $(6, 5)$.

It is interesting to note that in case of m being even but not divisible by 4 we have $(2^{m/2\pm1}+1)$ coprime to $(2^m - 1)$. Hence an argument on the lines of 2.6.3 was tried in the case of $(6, 5)$. More insight in this matter might be obtained if we have the

values of s for higher values of m, preferably $m = 10$. It is interesting to find out if these values correspond to a new class of permutation polynomial.

Chapter 3

Permutation Polynomials over $\mathbb{F}_{3m}$

3.1 Introduction

J.Yuan et al [6], considered the cases where the polynomial $p(x) = (x^3 - x + \delta)^s + x,\ Tr(\delta) \neq 0$ is a permutation polynomial over the field $\mathbb{F}_{3^m}$. The motivation for this work was the finding that over $\mathbb{F}_{3^m}$, the map

$x \rightarrow x - 1/x - 1/x^3$ is injective

This chapter is a review of the results obtained by them and a discussion of those results have been provided. The method adopted is similar to the one in previous chapter. A number of values of s such that $2 \leq s \leq 3^m - 2$ such that $p(x)$ is permutation polynomial are obtained by means of a MATLAB computer program. These values are given in the table 3.1 in section 3.2.

Afterwards theoretical explanations for the classification of these polynomials are provided in subsequent sections. This chapter contains 3 special classes of permutation polynomials, besides the linearized polynomials.

3.2 Computed values of s for different m

As in previous chapter, using a MATLAB program, designed for calculations over general odd prime finite fields, following values of s were obtained such that $(x^3 - x + \delta)^s + x$ is a permutation polynomial over $\mathbb{F}_{3^m}$. The values of interest are of course those lying in between 2 and $3^m - 2$.

Table 3.1: Values of s for which $(x^3 - x + \delta)^s + x$ permutes $\mathbb{F}_{3^m}$

m	*minimal polynomial*	δ	s
3	$x^3 - x + 1$	α^2	$3^a, 9^a, 11, 13^d, 16, 21^c, 24, 25^b$
4	$x^4 - x^3 - 1$	α	$9^a, 30, 40^d, 79^b$
5	$x^5 - x + 1$	α^4	$3^a, 9^a, 27^a, 81^a, 97^c, 121^d, 241^b$
6	$x^6 - x^4 + x^2 - x - 1$	α^2	$9^a, 81^a, 364^d, 727^b$

The values of s given in the table above are marked with letters indicating the section where the explanation of their permutation nature is provided. Corresponding to these values, subsequent sections contain proofs of these permutations.

3.3 Linearized permutation polynomial

As in previous chapter, first and foremost, we shall provide the values s which correspond to linearized polynomials over the field $\mathbb{F}_{3^m}$.

The values of s in the table marked with a are powers of 3 each of which give a linearized polynomial of the type:

$$x^{3^{k+1}} - x^{3^k} + x + \delta^{3^k}$$

A computer program given was used to verify if these linearized polynomials are also permutation polynomials under the condition of Theorem 1.4.2.
This covers values of s marked with a. We shall now proceed to some other classes of permutation polynomials.

3.4 Polynomials with $s = -1$

In this section, we discuss an important class of permutation polynomials over $\mathbb{F}_{3^m}$ namely $p(x),\ s = -1$. The polynomial then reduces to $\frac{1}{(x^3 - x + \delta)} + x$.
We shall now show that the equation

$$\frac{1}{(x^3 - x + \delta)} + x = a : \quad a \in \mathbb{F}_{3^m} \tag{3.4.1}$$

has a unique solution. This shall be proved by following theorem.

Theorem 3.4.1. *Let $\delta \in \mathbb{F}_{3^m}$ have non zero trace. Then the polynomial $\frac{1}{(x^3 - x + \delta)} + x$ is a permutation polynomial over $\mathbb{F}_{3^m}$.*

Proof. We shall prove that 3.4.1 has at most one solution for all a. Rearranging 3.4.1 as:

$$(x^3 - x + \delta)(x - a) + 1 = 0 \tag{3.4.2}$$

Putting $(x - a)$ as y, we have following equivalent equation:

$$y^4 - y^2 + (\delta - (a^3 - a))y + 1 = 0 \tag{3.4.3}$$

Let $b = (\delta - (a^3 - a))$.Then $Tr(b) = Tr(\delta) \neq 0$. Now we shall assume that above equation has 2 solutions,z and $(z+d)$. Then we have following set of equations:

$$z^4 - z^2 + bz + 1 = 0 \tag{3.4.4}$$

$$(z+d)^4 - (z+d)^2 + b(z+d) + 1 = 0 \tag{3.4.5}$$

Consider equation 3.4.5. It is equal to:

$$(z^4 - z^2 + bz + 1) + d(z^3 + (d^2+1)z + d^3 - d + b) = 0 \tag{3.4.6}$$

This reduces to

$$z^3 + (d^2+1)z + d^3 - d + b = 0 \tag{3.4.7}$$

From above it follows that $d \neq 0$ and $d^2 \neq 1$ since it would force $Tr(b) = 0$. Multiplying 3.4.7 by z and then subtracting 3.4.4 from it we get:

$$(d^2-1)z^2 + d(d^2-1)z - 1 = 0. \tag{3.4.8}$$

Dividing by z^2 throughout,we then have

$$\frac{1}{z^2} + 2d(d^2-1)\frac{1}{z} - (d^2-1) = 0$$

$$(1/z + (d^3 - d))^2 = (d^2-1)(d^2+1)^2$$

This means that $(d^2-1) = \beta^2$ for some $\beta \in \mathbb{F}_{3^m}$. Then

$$\begin{aligned}(d^2-1)(d^2+1)^2 &= \beta^2(\beta^2+2)^2 \\ = \beta^2(\beta^2-1)^2 &= (\beta^3-\beta)^2\end{aligned}$$

Hence $1/z = \pm(\beta^3-\beta)+(d^3-d)$. This means that the $Tr(1/z) = 0$. But $Tr(b) = Tr(-z^3+z+1/z) = Tr(1/z) \neq 0$. Hence we get a contradiction. So, our assumption that there are 2 solutions is wrong. This completes the proof of the theorem.

□

The class of permutation polynomials described above covers all the values that are marked with b in the table.

3.5 Polynomials with odd m

For certain odd integer values of m we obtain classes of permutation polynomials in which s is expressed as a function of m. It can be seen that the polynomial might be reduced to some known classes of basic permutation polynomials, in this case Dickson's polynomial of appropriate degree.

In this section we discuss two such classes of permutation polynomials over $\mathbb{F}_{3^m}$. The result, illustrated in subsequent theorem is due to Yuan et al [6].

Theorem 3.5.1. *Let $b \in \mathbb{F}_{3^m}$. If $m \equiv 3 \bmod 4$ then let $s = \frac{4.(3^m-1)+1}{5}$ and if $m \equiv 1 \bmod 4$ let $s = \frac{2(3^m-1)+1}{5}$. Then the polynomial $(x^3-x+\delta)^s + x$ when δ is an element with non zero trace in $\mathbb{F}_{3^m}$ is a permutation polynomial.*

Proof. We have following results:

when $m \equiv 3 \, mod \, 4$ then $\frac{4.(3^m-1)+1}{5} = 5^{-1} mod(3^m-1)$. Similarly, when $m \equiv 1 \, mod \, 4$ then $\frac{2.(3^m-1)+1}{5} = 5^{-1} mod(3^m - 1)$.

In either case the polynomial reduces to $(x^3 - x + \delta)^{5^{-1}} + x$. It suffices to prove that following equation has unique solution in $\mathbb{F}_{3^m}$.

$$(x^3 - x + \delta)^{5^{-1}} + x = a, \quad a \in \mathbb{F}_{3^m} \tag{3.5.1}$$

Since m is odd, $3^m - 1$ is coprime to 5. Hence

$$(x^3 - x + \delta) = (a - x)^5, \quad a \in \mathbb{F}_{3^m} \tag{3.5.2}$$

Replacing $(a - x)$ by y, we have

$$((a-y)^3 - (a-y) + \delta) = y^5 \tag{3.5.3}$$

$$y^5 + y^3 - y = a^3 - a + \delta \tag{3.5.4}$$

Above polynomial is a Dickson's polynomial of degree 5 [4]. Since 5 is coprime to $(3^{2m} - 1)$, it is also a permutation polynomial, by theorem 1.4.3. This ends the proof of the theorem. □

The values of s in table marked with c are the ones which lie in this class of permutation polynomials. A similar approach is taken to create classes for higher prime fields in next chapter. A analogous result however doesn't exist for even values of m.

3.6 A special class of permutation polynomials

In this section, a general class of permutation polynomial is obtained which is based on the property of $L(x)$ a linearized polynomial being a linear operator of $\mathbb{F}_{3^m}$ taken as a vector space over base field.

We shall prove a theorem below and then see that a polynomial of kind we have considered satisfies the condition of the theorem.

Theorem 3.6.1. *Let $h(x)$ be a function defined over $\mathbb{F}_{p^m}$. Let $L(x)$ be a linearized polynomial over $\mathbb{F}_{p^m}$ such that for any $a,\ b \in \mathbb{F}_{p^m}$, we have $h(a) - h(b) \in ker(L) = \{x \in \mathbb{F}_{p^m} | L(x) = 0\}$. Then $f(x) = h(L(x) + c) + x$ is a permutation polynomial of $\mathbb{F}_{p^m}$ for any $c \in \mathbb{F}_{p^m}$.*

Proof. Assume there exist $x,\ y \in \mathbb{F}_{p^m}$ such that $f(x) = f(y)$. Then we have $x - y = h(L(y) + c) - h(L(x) + c) \in ker(L)$. So $L(x) = L(y)$, which in turn implies $x - y = h(L(y) + c) - h(L(x) + c) = 0$. Hence f is a permutation over $\mathbb{F}_{p^m}$. This completes the proof of the theorem.

□

We shall now use above theorem to prove certain polynomials to be permutation polynomials. Now assume $s = \frac{(3^m - 1)}{2}$. Then $3s \equiv s \ mod\ (3^m - 1)$. Also consider the function $h(x) = x^s$ and $L(x) = x^3 - x$. Under these conditions assume $h(a) - h(b) = x$. We see that

$$\begin{aligned} L(x) &= L(a^s - b^s) \\ &= (a^s - b^s)^3 - (a^s - b^s) \\ &= (a^{3s} - b^{3s}) - (a^s - b^s) \\ &= (a^s - b^s) - (a^s - b^s) \\ &= 0 \end{aligned}$$

Hence, $h(x)$ satisfies the conditions of the theorem. So, $f(x) = (x^3 - x + \delta)^s + x$ is a permutation polynomial when $s = \frac{(3^m - 1)}{2}$. The values of s in the table marked d are the ones which fall under this class.

It is to be mentioned that an alternative proof for these polynomials has also been provided which creates a class that includes these polynomials also. We shall mention in detail that proof in next chapter.

3.7 Conclusion

This chapter is a detailed survey of known classes of permutation polynomial of the type $p(x) = (x^3 - x + \delta)^s + x$, $Tr(\delta) \neq 0$ over the field $\mathbb{F}_{3^m}$. Most of the results included in this chapter are due to Yuan et al [6]. However, we have tried to reconstruct the proofs in section 3.4 and 3.6 in a more comprehensible way. Especially, we have not resorted to the arguments using quadratic residues in section 3.6 but presented a more neat calculation based proof.

It is observed that certain values of s still need to be classified from the table. It would be interesting to find if they give rise to any new classes of polynomials.

Few ideas from this chapter are continued to next one in obtaining some new classes of permutation polynomials.

Chapter 4

New classes of Permutation Polynomials over $\mathbb{F}_{5^m}$

4.1 Introduction

The results discussed in previous chapters provide a motivation to search for similar results in the case of finite fields with base prime 5. In this chapter, we shall embark upon similar methods of searching computationally, the existence of permutation polynomials over field $\mathbb{F}_{5^m}$.

Our interest is in the values s such that $2 \leq s \leq 5^m - 2$ and $(x^5 - x + \delta)^s + x$ is a permutation polynomial over $\mathbb{F}_{5^m}$ for δ an element of $\mathbb{F}_{5^m}$ with non-zero trace. Using the computer program, which was used in previous chapter, various such values are obtained for different values of m. These values are listed in the table 4.1 given in the section 4.2.

This chapter contains certain new classes of permutation polynomials, which explains various values of s obtained. Some of the values are as yet not classified while a few

can be shown to belong to no class but to be default values for permutation polynomial. All of these values have been accordingly discussed.

Additionally, to obtain a better perception of classes of permutation polynomials over $\mathbb{F}_{5^m}$ and to avoid computational limitations, the values of s have also been obtained for the $m = 2$.

4.2 Computed values of s for different m

As in previous chapter, using a MATLAB program, designed for calculations over general odd prime finite fields, following values of s are obtained such that $(x^5 - x + \delta)^s + x$ is a permutation polynomial over $\mathbb{F}_{5^m}$. The values of interest are of course those lying in between 2 and $5^m - 2$.

Table 4.1: Values of s for which $(x^5 - x + \delta)^s + x$ permutes $\mathbb{F}_{5^m}$

m	*minimal polynomial*	δ	s
2	$2x^2 + x + 1$	α^0	2^b , 3 , 5^a, 6^c, 12^c, 18^c, 19
3	$2x^3 + 3x^2 + 1$	α^0	5^a , 21 , 25^a , 31^c , 62^c , 67 , 83^d , 93^c
4	$2x^4 + 2x^3 + x^2 + 1$	α^0	5^a , 26 , 156^c , 312^c , 468^c

The values of s given in the table above are marked with letters indicating the section where the explanation of their permutation nature is provided. Corresponding to them, subsequent sections contain explanations for these values.

4.3 Linearized permutation polynomials

As in previous chapters, first and foremost, we shall provide the values s which correspond to linearized polynomials over the field $\mathbb{F}_{5^m}$.

The values of s in the table marked with a are powers of 5 each of which give a linearized polynomial of the type:

$$x^{5^{k+1}} - x^{5^k} + x + \delta^{5^k}$$

A MATLAB computer program can check if these linearized polynomials are also permutation polynomials under the condition of theorem 1.4.2. It turns out that these are the only values which give linearized permutation polynomials.

This covers values of s marked with a.

4.4 Nature of $(x^p - x + \delta)^2 + x$

In this section, we shall prove that $(x^p - x + \delta)^2 + x$ is always a permutation polynomial over field $\mathbb{F}_{p^2}$. We start by stating the following lemma.

Lemma 4.4.1. *Polynomial $(x^p - x + \delta)^2 + x$ over the finite field $\mathbb{F}_{p^2}$, δ is an element of the field with non-zero trace, is a permutation polynomial*

Proof. The polynomial $(x^p - x + \delta)^2 + x$ over the finite field $\mathbb{F}_{p^2}$ is a permutation polynomial if and only if following equation has only one solution.

$$(x^p - x + \delta)^2 + x = d \tag{4.4.1}$$

for some d, element of the field $\mathbb{F}_{p^2}$.

This means,

$$(x^p - x + \delta)^2 = (d - x) \tag{4.4.2}$$

has only one solution. Raising both sides to the power of p since p is coprime to $p^2 - 1$, the resultant is still a permutation polynomial. Hence,

$$(x^p - x + \delta)^{2p} = (d-x)^p \tag{4.4.3}$$

$$(x^{p^2} - x^p + \delta^p)^2 = (d-x)^p \tag{4.4.4}$$

$$(x - x^p + \delta^p)^2 = (d-x)^p \tag{4.4.5}$$

has only one solution.

Substituting $(d-x) = y$ we get;

$$[d^p - d + \delta - (y^p - y)]^2 = y \tag{4.4.6}$$

$$(c_1 - (y^p - y))^2 = y \tag{4.4.7}$$

in place of 4.4.2 and

$$[d^p - d - \delta^p - (y^p - y)]^2 = y^p \tag{4.4.8}$$

$$(c_2 - (y^p - y))^2 = y^p \tag{4.4.9}$$

in place of 4.4.5.

Substituting $(y^p - y) = z$ and substracting 4.4.7 from 4.4.9, we get;

$$(c_1 - z)^2 - (c_2 - z)^2 = z \tag{4.4.10}$$

$$(c_1 - c_2)(c_1 + c_2 - 2z) = z \tag{4.4.11}$$

$$(1 + 2(c_1 - c_2))z = c_1^2 - c_2^2 \tag{4.4.12}$$

$$z = \frac{c_1^2 - c_2^2}{1 + 2(c_1 - c_2)} \tag{4.4.13}$$

Substituting this value of $(y^p - y) = z$ in 4.4.7, we get

$$y = [c_1 + \frac{c_1^2 - c_2^2}{1 + 2(c_1 - c_2)}]^2 \tag{4.4.14}$$

Since, all the quantities on right hand of the equation are constants, it is clear that for some unique d, value of y and hence x is unique. This proves that the polynomial $(x^p - x + \delta)^2 + x$ over the finite field $\mathbb{F}_{p^2}$, δ is an element of the field with non-zero trace, is a permutation polynomial. □

Values of s in the table that are marked b are explained in this section. Since this proof does not take into account the base prime of the finite field hence it is evidently true for all finite fields.

Next section deals with a another class of polynomials which again is not dependent upon the base prime of the field.

4.5 Polynomials with $s = \frac{k(p^m - 1)}{p - 1}$ over $\mathbb{F}_{p^m}$

If the polynomial $(x^5 - x + \delta)^s + x$ with δ an element of $\mathbb{F}_{5^m}$ with non-zero trace, is such that $s = \frac{k(5^m - 1)}{4}$, $k = 0, 1, 2, 3$, then it is possible to establish their permutation property under the following general theorem.

The result makes use of following lemma about elements of finite fields.

Lemma 4.5.1. *Let x be an element of finite field $\mathbb{F}_{p^m}$. Then $x^s = x^{ps}$, where $s = \frac{k(p^m - 1)}{p - 1}$,$k \in [0, 1, 2, ..., p - 2]$.*

Proof. The proof requires nothing more than a restructuring of the expression for s.

$$\begin{aligned} ps &= \frac{(p^m - 1)(p - 1 + 1)k}{p-1} \\ ps &= k(p^m - 1) + \frac{(p^m - 1)k}{p-1} \end{aligned}$$

Hence, it follows,

$$\begin{aligned} x^{ps} &= x^{k(p^m - 1)}.x^{\frac{(p^m - 1)k}{p-1}} \\ x^{ps} &= 1.x^s \end{aligned}$$

This proves the lemma. □

We shall now state the main theorem and provide a proof for the same.

Theorem 4.5.2. *If* $s = \frac{k(p^m - 1)}{p - 1}$ *and* δ *is an element of the field* $\mathbb{F}_{p^m}$ *with its trace non zero, then the polynomial* $(x^p - x + \delta)^s + x$ *is a permutation polynomial over the same finite field.*

Proof. Given polynomial is a permutation polynomial if and only if the following equation has not more than single solution in the given finite field.

$$[x^p - x + \delta]^s + x = d \tag{4.5.1}$$

for some element d in the field.

Transferring x to left hand side and substituting $(d - x) = y$ we get following equation

$$[d^p - d + \delta - (y^p - y)]^s = y \tag{4.5.2}$$

Raising on both sides to power of p, since p is coprime to $(p^m - 1)$ we get following,

$$[d^p - d + \delta - (y^p - y)]^{ps} = y^p \tag{4.5.3}$$

From Lemma 4.5.1 and eqn 4.5.2, we get $y^p = y$.

This means that $(y^{(p-1)} - 1)(y) = 0$. However, if $y = (d - x) = 0$, then polynomial $[x^p - x + \delta]$ must have a root in the field. However, this polynomial is irreducible for all values of p as $Tr(\delta)$ is non zero.

So we can conclude that, $y^{(p-1)} - 1 = 0$.

Only possible solutions of this equation are

$$y = \alpha^{\frac{i(p^m - 1)}{p-1}} \quad ; i = 0, 1, 2, .., (p - 1)$$

where α is a primitive element of the field. Putting back $x = d - \alpha^{\frac{i(p^m - 1)}{p-1}}$ in eqn.4.5.1, we get the following

$$[d^p - d + \delta - (\alpha^{\frac{ip(p^m - 1)}{p-1}} - \alpha^{\frac{i(p^m - 1)}{p-1}})] = \alpha^{\frac{i(p^m - 1)}{p-1}}$$

By Lemma 4.5.1

$\alpha^{\frac{pi(p^m - 1)}{p-1}} = \alpha^{\frac{i(p^m - 1)}{p-1}}$

hence we have

$$[d^p - d + \delta] = \alpha^{\frac{i(p^m - 1)}{p-1}}$$

Since, the right hand side is a constant, it means for a given d, there can be only one possible value of i that can be chosen. Hence, eqn 4.5.1 has at most a single solution. So the polynomial is a permutation polynomial. □

It must be stated that choosing different values of k we can have $p - 2$ different values of s, excluding the obvious choices of 0 and $p - 1$, which give rise to permutation polynomials over finite fields. The values of s in the table that are marked c

are covered under this class of polynomials.

Also it is notable that in previous chapters certain polynomials fall under this class besides their given classification. However, for prime $p = 2$, class is trivial. Under $p = 3$, this class explains single polynomials for each value of m which are explained otherwise.

The size of this class however increases with the value of base prime and as such it is a simple but important class of polynomials.

In the next section we discuss an important class of permutation polynomial based on the nature of m.

4.6 Permutation polynomial over $\mathbb{F}_{5^{2k+1}}$

In previous chapters we observed that if we know whether m is an odd or even number, we can provide certain expressions for s in terms of p and m such that the resultant polynomial is a permutation polynomial. Many such classes of polynomials have been discussed previously.

In this section, we provide such a class of permutation polynomial for the case when m is an odd integer.

Theorem 4.6.1. *Let $m = 2k + 1$ be an odd integer. Then for $s = \frac{2.5^m - 1}{3}$ the polynomial $(x^5 - x + \delta)^s + x$ is a permutation polynomial over $\mathbb{F}_{5^m}$.*

Proof. Consider $s = \frac{2.5^m - 1}{3}$. Then;

$$3s = 2(5^m - 1) + 1 = 1 mod(5^m - 1)$$
$$s = \frac{1}{3} mod(5^m - 1)$$

For odd m 3 is coprime to $(5^m - 1)$. We need to show that the equation $(x^5 - x + \delta)^s + x = d$ has atmost a single solution in the given finite field, in order to show that it is a permutation polynomial.

Taking the equation and raising both sides to power of 3, we get;

$$(x^5 - x + \delta)^{1/3} = (d - x) \tag{4.6.1}$$
$$(x^5 - x + \delta) = (d - x)^3 \tag{4.6.2}$$

Taking $(x - d) = y$ we obtain following;

$$y^5 - y + d^5 - d + \delta = -y^3 \tag{4.6.3}$$
$$y^5 + y^3 - y = d - d^5 - \delta = b \tag{4.6.4}$$

Above polynomial, as in previous chapter is, a Dickson's polynomial. Since 5 is coprime to $5^{2m} - 1$, it is also a permutation polynomial by theorem 1.4.3. Hence given polynomial permutes the elements of the finite field. □

In the table the values marked as d are covered by this class.

4.7 Conclusion

This chapter includes some novel and as yet unknown classes of permutation polynomials. It can, however, be observed that still some values obtained computationally,

don't fall under any of these classes.

We also saw that it is possible for one polynomial to be the only representative of its class. Consequently, it would be a matter of further inquiry as to whether the remaining values of the s in the table give rise to any new class of polynomials or is the lone member of its own class.

In case of the section 4.5, we observed that the key step was establishing the fact that $x^p - x$ is independent of x and is a constant. Hopefully, this could be an useful technique for further research in this area.

Appendix

4.8 Used MATLAB Programs

1.For even prime

```
    m = input('m=')
for i= 2:2^m-1
    x = gf(i,m);
    sum = gf(0,m);
    for k = 0:m-1
        sum = sum + x^(2^k);
    end
    if (sum == 1)
        delta = x;
        break
    end
end
delta

p = 1;
for s = 0:2^m-1
    for n = 1:2^m
        c(n)= 0;
    end
    for i= 0:2^m-1
        x = gf(i,m);
        d = (x^2 + x + delta)^s;
        o_poly = 1/d + x;

        for j = 0:2^m-1
            if (o_poly == gf(j,m))
                c(j+1)= c(j+1)+1;
            end
        end
    end
    l= 0;
    for k = 1:2^m
        if (c(k)==1)
            l= l+1;
        end
    end
    if (l==2^m)
        s_array(p) = s;
        p = p+1;
```

```
    end
end
s_array
```

2.For odd primes

```
clear all
clc

p = input('prime=');
m = input('index=');
field = gftuple([-1:p^m-2]',m,p);
prim_poly = gfprimdf(m,p)

for i = -1:p^m-2
    trace = i;
    for j = 1:m-1
        x = gfmul(i,i,field);
        for k = 1:p^j-2
            x = gfmul(x,i,field);
        end
        trace = gfadd(trace,x,field);
    end
    if(trace > 0)
        d = i;
        break
    end
end
d
t = 1;
%s = input('s=');
for s = 2:p^m-2
k = 1;
for i = -1:p^m-2
    x = gfmul(i,i,field);
    for mu = 1:p-2
    x = gfmul(x,i,field);
    end
    y = gfsub(x,i,field);
    z = gfadd(y,d,field);
    w = gfmul(z,z,field);
    for j = 1:s-2
        w = gfmul(w,z,field);
    end
    poly(k) = gfadd(w,i,field);
    k = k+1;
end
poly;
r = 0;
for k = 1:p^m
    for j = 1:p^m
        if (poly(k)== poly(j) & k~=j)
            break
        else
            r = r+1;
        end
    end
```

```
end
if (r == p^(2*m))
    s_array(t)= s;
    t = t+1;
    %'yes'
end
end
s_array
```

Bibliography

[1] R.S. Coulter, *On evaluation of a class of weil sums in characteristic 2*, New Zealand Journal of Mathematics **28** (1999), 171–184.

[2] T. Helleseth and V. Zinoviev, *New kloosterman sums identities over* $\mathbb{F}_{2^m}$ *for all* m, Finite Fields and their Applications **9** (2003), 187–193.

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

[4] G. Turnwald R. Lidl, G.L. Mullen (ed.), *Dickson's polynomials*, vol. 14, Longman, New York, 1993.

[5] J. Yuan and C. Ding, *Four classes of permutation polynomials of* $\mathbb{F}_{2^m}$, Finite Fields and their Applications **13** (2006), 869–876.

[6] Jin Yuan and Cunsheng Ding, *Permutation polynomials of the form* $(x^p - x + \delta)^s + l(x)$, Finite Fields and their Applications **14** (2008), 482–493.