ON PERMUTATION POLYNOMIALS OVER FINITE FIELDS

ROHIT GUPTA

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
JUNE 2018

ON PERMUTATION POLYNOMIALS OVER FINITE FIELDS

by

ROHIT GUPTA

Department of Mathematics

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Delhi

June 2018

Dedicated to

My Family

Certificate

This is to certify that the thesis entitled **"On Permutation Polynomials over Finite Fields"** submitted by **"Mr. Rohit Gupta"** to the Indian Institute of Technology Delhi, for the award of the Degree of **Doctor of Philosophy**, is a record of the original bona fide research work carried out by him under my guidance and supervision. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

New Delhi
June 2018

Dr. R. K. Sharma
Professor
Department of Mathematics
Indian Institute of Technology Delhi

Acknowledgements

It gives me great pleasure to express my sincere gratitude to my supervisor, Prof. R. K. Sharma, for his constant encouragement and the freedom he gave me while working on my thesis. His ardent dedication to perfection, exactness and completeness inspired me to write this thesis as good as possible. His suggestions on the manuscript have helped me to improve the quality of this thesis.

I would like to extend my appreciation to my SRC (Student Research Committee) members Prof. Aparna Mehra, Dr. Ritumoni Sarma and Prof. O. P. Gandhi for their valuable time and suggestions. I am greatly indebted to all faculty members of Department of Mathematics IIT Delhi, for their coopration and support. Also I would like to thank CSIR (Council of Scientific and Industrial Research) for providing me the financial assistance during the period of my research work.

I appreciate all my seniors for making me comfortable in the department and motivating me in the initial days of my research. I would like to give my heartily thanks to Dr. Alok Mishra and Dr. Amit Kumar Sharma. It appears almost impossible to thank each one of my friends here individually, but I would like them to know that the happy memories of my friendship with them always remain in the deepest corner of my heart. I am highly thankful to my colleagues and friends, Pawan, Rahul, Chirag, Satya, Deep Chandra, Anuj, Yogesh, Vishal, for encouraging me and creating joyful environment in this duration.

Words cannot completely express my love and gratitude to my family who have supported and encouraged me through this journey. I would like to thank my parents for their life long support which sustained my interest in research and motivated me towards the successful completion of this study.

Finally, and most importantly, I would like to thank my wife Ankita Jindal. Her support, encouragement and quiet patience were undeniably the bedrock upon which the past few years of my life have been built.

Last but not the least, I would like to thank the Almighty God for being with me and answering all my prayers.

New Delhi *Rohit Gupta*

June 2018

Abstract

This thesis is devoted to the study of certain types of permuation polynomials over finite fields. Permutation polynomials have applications in many diverse fields of mathematics. In this thesis, we are generally concerned with the following question: Given a polynomial $f(x) \in \mathbb{F}_q[x]$, when does the map $x \to f(x)$ induce a permutation on $\mathbb{F}_q$?

There is an aesthetic appeal of binomials and trinomials that permute finite fields. Despite of the simplest algebraic form, these polynomials permute finite fields for highly nontrivial reasons. In this thesis, we study binomials and trinomials of the form $x^r h(x^{q+1}) \in \mathbb{F}_{q^2}[x]$. We give explicit conditions on the coefficients of these polynomials to attain permutation property for certain values of r and for some choices of $h(x) \in \mathbb{F}_{q^2}[x]$. Apart from the above mentioned permutation trinomials, we also present four classes of permutation trinomials of this form $x^r h(x^{2^m-1}) \in \mathbb{F}_{2^{2m}}[x]$ with trivial coefficients.

In this thesis, we also study permutation polynomials of the form $(x^{p^m}-x+\delta)^s+x$ over $\mathbb{F}_{p^{2m}}$. More precisely, we consider the case when $p \in \{2,3\}$ and by determining the number of solutions of certain equations over a given finite field, we obtain two new classes of permutation polynomials of the form $(x^{2^m}+x+\delta)^{i(2^m-1)+1}+x$ over $\mathbb{F}_{2^{2m}}$ and one new class of permutation polynomials of the form $(x^{3^m}-x+\delta)^{i(3^m-1)+1}+x$ over $\mathbb{F}_{3^{2m}}$.

We also study o-polynomials in this thesis. These polynomials are a particular type of permutation polynomials which have applications in finite projecive planes. Towards the end, we classify all o-polynomials up to degree 8.

सार

यह शोध परिमित क्षेत्रो मे कुछ प्रकार के क्रमचय बहुपदो के अध्ययन के लिए समर्पित है। क्रमचय बहुपदो के अंकशास्त्र के कई विविध क्षेत्रो मे अनुप्रयोग हैं। इस शोध मे, हम आम तौर पर निम्नलिखित प्रश्न से सम्बध्द हैं: दिये गये बहुपद $f(x) \in \mathbb{F}_q[x]$ के लिए, कब फलन $x \longrightarrow f(x)$, $\mathbb{F}_q$ पर एक क्रमचय को उत्पन्न करता है?

जो परिमित क्षेत्रो के लिए क्रमचय हैं, ऐसे द्विपदो और त्रिपदो का सौन्द्र्यात्मक आकर्षण है। ये बहुपद सबसे सरल बीजगणितीय रूप के हैं, फिर भी अत्यधिक गैर तुच्छ कारणों से ये परिमित क्षेत्रो के लिए क्रमचय हैं। इस शोध मे, हम $x^r h(x^{q+1}) \in \mathbb{F}_{q^2}[x]$ के रूप के द्विपदो और त्रिपदो का अध्ययन करते हैं। हम r के कुछ मानो के लिए और $h(x) \in \mathbb{F}_{q^2}[x]$ के कुछ विकल्पो के लिए इन बहुपद के गुणांक पर स्पष्ट शर्ते देते हैं जिससे की ये बहुपद क्रमचय के गुण को ग्रहण करें। उपरोक्त वर्णित त्रिपदो के अलावा, हम तुच्छ गुणांको के साथ $x^r h(x^{2^m-1}) \in \mathbb{F}_{2^{2m}}[x]$ के रूप के चार क्रमचय त्रिपदो को भी प्रस्तुत करते हैं।

इस शोध मे, हम $(x^{p^m} - x + \delta)^s + x \in \mathbb{F}_{p^{2m}}[x]$ के रूप के क्रमचय बहुपदो का भी अध्ययन करते हैं। स्पष्ट रूप मे, हम $p \in \{2,3\}$ मामले पर विचार करते हैं और परिमित क्षेत्रो पर कुछ समीकरणो के समाधानो की संख्या निकालकर, हम $(x^{p^m} - x + \delta)^{i(2^m-1)+1} + x \in \mathbb{F}_{2^{2m}}[x]$ के रूप की क्रमचय बहुपदो की दो नई श्रेणी और $(x^{p^m} - x + \delta)^{i(3^m-1)+1} + x \in \mathbb{F}_{3^{2m}}[x]$ के रूप की क्रमचय बहुपदो की एक नई श्रेणी प्राप्त करते हैं।

इस शोध मे हम ०-बहुपदो का भी अध्ययन करते हैं। ये बहुपद एक विशेष प्रकार के क्रमचय बहुपद हैं जिनका अनुप्रयोग सीमित प्रक्षेपित सतहो मे होता है। इसके अंत मे, हम 8 घात तक के सारे ०-बहुपदो को वर्गीकृत करते हैं।

Contents