PERMUTATION POLYNOMIALS OVER FINITE FIELDS AND FINITE GROUP RINGS

POOJA

DEPARTMENT OF MATHEMATICS

INDIAN INSTITUTE OF TECHNOLOGY DELHI

JULY 2023

PERMUTATION POLYNOMIALS OVER FINITE FIELDS AND FINITE GROUP RINGS

by

POOJA

Department of Mathematics

Submitted

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

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI

JULY 2023

Dedicated to

My Daughter

Certificate

This is to certify that the thesis entitled **"Permutation Polynomials over Finite Fields and Finite Group Rings"** submitted by **"Ms. Pooja"** to the Indian Institute of Technology Delhi, for the award of the degree of **Doctor of Philosophy**, is a record of the original bonafide research work carried out by her under my supervision and guidance. 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.

Dr. R. K. Sharma
Professor
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi, 110016

New Delhi
July 2023

Acknowledgements

It gives me immense pleasure to express my sincere gratitude to various persons who have helped and inspired me throughout my Ph.D. First and foremost, I would like to praise God, the almighty, for giving me countless blessing, strength and opportunity so that I have been able to accomplish the thesis.

It is with a deep sense of regard and respect that I acknowledge my deepest gratitude to my supervisor, Prof. R. K. Sharma, for his continuous advice and support. His constant encouragement, ardent dedication to perfection and valuable suggestions during all the stages of my research work helps me to write thesis as good as possible.

I would like to extend my sincere gratitude to my SRC (Student Research Committee) members Prof. Ritumoni Sarma, Prof. Amit Priyadarshi and Prof. R.K. Varshney for their co-operation, inspiration, valuable time and useful suggestions. I am greatly obliged to all the faculty members of Department of Mathematics, IIT Delhi, for their co-operation and support. I would also like to thank UGC(University Grants Commission)for providing me financial assistance and IIT Delhi authorities for providing all the necessary facilities required during my research work.

I appreciate all my seniors for making me comfortable in the department and motivating in the initial days of my research. I would like to give my warm and sincere thanks to my co-author Dr. Rohit Gupta for his support and guidance whenever I approached him for the same. His valuable suggestions on the manuscripts helped me a lot. I would like to give my heartily thanks to my friend Soniya Takshak for her unconditional love and support. It was an amazing time with her during my Ph.D. Joyful memories of our friendship will always be in my heart. I am highly thankful to my seniors, colleagues and friends, Archna, Astha, Divya, Neha, Praveen, Sonika, Sonamani, Surbhi, Dhiraj, Gyanendra, Mohit for encouraging me and creating joyful environment during this time. 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 remains in the deepest corner of my heart.

Words are not enough to express my love and gratitude to my family who have always supported and encouraged me in every phase of my life. I am forever indebted

to my parents for giving me the opportunities and experiences that have made me who I am. All my achievements are outcomes of the silent sacrifice and patience of my parents. Also I express my thanks to my brother Rohit, and sister Sonia for their constant support and valuable prayers.

Finally, and most importantly, I would like to thank my husband Ravit Malik for his continuous love, unconditional support and understanding during my pursuit of Ph.D degree. His encouragement and quiet patience were undeniably the bedrock upon which the past one and half year of my life has been built.

New Delhi *Pooja*
July 2023

Abstract

Let R denotes a finite commutative ring. A polynomial $f(x) \in R[x]$ is said to be a *permutation polynomial* over $\mathbb{F}_q$ if the associated polynomial function $f : c \to f(c)$ from R into R is a permutation of R. This thesis is dedicated to the study of specific types of permutation polynomials over finite fields and finite group rings. Permutation polynomials have various applications in distinct areas of mathematics. We are mainly concerned with the question that given $f(x) \in S[x]$ where S can be a finite field or finite group ring, when does the mapping $x \to f(x)$ induce a permutation on S?

In this thesis, we study permutation trinomials over $\mathbb{F}_{q^3}$ of the form $f(x) = x^d + L(x^s)$ by choosing some suitable integers d, s and a linearized polynomial $L(x)$ i.e. A polynomial for which exponents of all constituent monomials are powers of q and coefficients come from some extension field of the finite field of order q. In general, it is difficult to study permutation trinomials over $\mathbb{F}_{q^3}$. In fact, it can be seen in the literature that the coefficients of most of the so far known permutation trinomials are all 1. For $d = 1$ and for different linearized polynomials $L(x)$, we give explicit conditions on the coefficients of these polynomials to become permutation polynomials. More precisely, we propose three new classes of permutation trinomials over $\mathbb{F}_{q^3}$ in chapter 3. Among these classes, the first two classes are $x + Ax^{q^2-q+1} + x^{q^2+q-1}$(Theorem 3.4.1) and $x + Ax^{q^3-q^2+q} + x^{q^2+q-1}$(Theorem 3.4.2), q even and the third class is $x + Ax^{q^2-q+1} + A^2x^{q^2}$(Theorem 3.5.1), q odd. We also prove a conjecture given by [13] as a particular case of our results.

In this thesis, we also investigate permutation behavior of polynomials over $\mathbb{F}_{p^{2m}}$ of the form $(x^{p^m} - x + \delta)^s + L(x)$ and $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + L(x)$, where $L(x)$ is a linearized polynomial. More precisely, using a method based on criterion given by Akbary et. al. (AGW Criterion) and by determining the number of solutions of certain lower degree equations in a subset of $\mathbb{F}_{p^{2m}}$, three classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$(Theorem 4.2.1, Theorem 4.2.4 and Theorem 4.2.5) and three classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + L(x)$ (Theorem 4.2.2, Theorem 4.2.3 and Theorem 4.2.6) over the finite field $\mathbb{F}_{p^{2m}}$ are given, where $p = 3$ or $p = 5$, $L(x) = ax^{p^m} + ax$

and $a \in \mathbb{F}_{p^m}^*$.

Also, we further extended the study of permutation behavior of polynomials of same form and propose seven classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$(Theorem 5.2.1) and $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + L(x)$ (Theorem 5.3.1, Theorem 5.3.2, Theorem 5.3.3, Theorem 5.3.4, Theorem 5.3.5 and Theorem 5.3.6) over $\mathbb{F}_{p^{2m}}$, where $L(x) = x$ and $p = 5$. Determination of number of solutions of some lower degree equations in a subset of $\mathbb{F}_{p^{2m}}$ plays a key role in our constructions.

Further, permutation polynomials over R have many applications in cryptography and coding theory mostly when R is a field. There is some study for permutation polynomials over residue class rings. But picture is not so clear for arbitrary commutative rings. We also study permutation polynomials over finite group rings in this thesis and give a class of permutation polynomial over the group ring $F_pC_{p^n}$(Theorem 6.2.1).

सार

माना R एक परिमित क्रमविनिमेय वलय को दर्शाता है। एक बहुपद $f(x) \in R[x]$ को $\mathbb{F}_q$ पर एक क्रमपरिवर्तन बहुपद कहा जाता है यदि संबद्ध बहुपद फलन $f: c \to f(c),\ R$ से R तक R का क्रमपरिवर्तन है। यह शोध प्रबंध परिमित क्षेत्रों और परिमित समूह वलय पर विशिष्ट प्रकार के क्रमपरिवर्तन बहुपदों के अध्ययन के लिए समर्पित है। गणित के विभिन्न क्षेत्रों में क्रमपरिवर्तन बहुपदों के विभिन्न अनुप्रयोग होते हैं। हमें मुख्य रूप से इस प्रश्न से संबद्ध हैं कि दिया गया $f(x) \in S[x]$ जहां S एक परिमित क्षेत्र या परिमित समूह वलय हो सकता है, मैपिंग $x \to f(x),\ S$ पर क्रमपरिवर्तन कब प्रेरित करती है?

इस शोध प्रबंध में, हम $\mathbb{F}_{q^3}$ पर कुछ उपयुक्त पूर्णांक d, s और एक रैखिककृत बहुपद $L(x)$ चुनकर $f(x) = x^d + L(x^s)$ प्रकार की क्रमपरिवर्तन त्रिपदों का अध्ययन करते हैं यानी एक बहुपद जिसके सभी एकपदी घटक के घातांक q की घातें हैं और गुणांक q क्रम के परिमित क्षेत्र के किसी विस्तार क्षेत्र से आते हैं। सामान्यतः $\mathbb{F}_{q^3}$ पर क्रमपरिवर्तन त्रिपदों का अध्ययन करना कठिन है। वास्तव में, साहित्य में देखा सकता है कि अब तक ज्ञात अधिकांश सभी क्रमपरिवर्तन त्रिपदों के गुणांक 1 हैं। $d = 1$ और विभिन्न रैखिककृत बहुपदों $L(x)$ के लिए, हमने क्रमपरिवर्तन बहुपद बनने के लिए इन बहुपदों के गुणांकों पर स्पष्ट शर्तें दी हैं। अधिक सटीक रूप से, अध्याय 3 में हमने $\mathbb{F}_{q^3}$ पर क्रमपरिवर्तन त्रिपदों के तीन नए वर्गों का प्रस्ताव दिया है। इन वर्गों में से, पहले दो वर्ग $x + Ax^{q^2-q+1} + x^{q^2+q-1}$ (प्रमेय 3.4.1) और $x + Ax^{q^3-q^2+q} + x^{q^2+q-1}$ (प्रमेय 3.4.2), q सम हैं और तीसरा वर्ग $x + Ax^{q^2-q+1} + A^2 x^{q^2}$ (प्रमेय 3.5.1), q विषम है । हमारे परिणामों के एक विशेष मामले के रूप में हम [13] द्वारा दिया गया अनुमान भी साबित करते हैं।

इस शोध प्रबंध में, हम $\mathbb{F}_{p^{2m}}$ पर $(x^{p^m} - \mathrm{x} + \delta)^s + L(x)$ और $(x^{p^m} - \mathrm{x} + \delta)^{s_1} + (x^{p^m} - \mathrm{x} + \delta)^{s_2} + L(x)$, जहाँ $L(x)$ एक रैखिककृत बहुपद है, प्रकार के बहुपदों के क्रमपरिवर्तन व्यवहार की भी जांच करते हैं। अधिक सटीक से, अकबरी एट अल. द्वारा दिए गए मानदंड (एजीडब्ल्यू मानदंड) पर आधारित एक विधि का उपयोग करके और $\mathbb{F}_{p^{2m}}$ के एक उपसमुच्चय में कुछ निम्न डिग्री समीकरणों के समाधान संख्या निर्धारित करके, $(x^{p^m} - \mathrm{x} + \delta)^s + L(x)$ प्रकार के क्रमपरिवर्तन बहुपद के तीन वर्ग (प्रमेय 4.2.1, प्रमेय 4.2.4 और प्रमेय 4.2.5) और $(x^{p^m} - \mathrm{x} + \delta)^{s_1} + (x^{p^m} - \mathrm{x} + \delta)^{s_2} + L(x)$ प्रकार के क्रमपरिवर्तन बहुपद के तीन वर्ग (प्रमेय 4.2.2, प्रमेय 4.2.3 और प्रमेय 4.2.6) परिमित क्षेत्र $\mathbb{F}_{p^{2m}}$ पर दिए गए हैं, जहां $p = 3$ या $p = 5$, $L(x) = ax^{p^m} + ax$ और $a \in \mathbb{F}_q^*$ हैं।

साथ ही, हमने इसी रूप के बहुपदों के क्रमपरिवर्तन व्यवहार के अध्ययन को और आगे बढ़ाया और $\mathbb{F}_{p^{2m}}$ पर $(x^{p^m} - \mathrm{x} + \delta)^s + L(x)$ (प्रमेय 5.2.1) और $(x^{p^m} - \mathrm{x} + \delta)^{s_1} + (x^{p^m} - \mathrm{x} + \delta)^{s_2} + L(x)$ (प्रमेय 5.3.1, प्रमेय 5.3.2, प्रमेय 5.3.3, प्रमेय 5.3.4, प्रमेय 5.3.5 और प्रमेय 5.3.6) प्रकार

के क्रमपरिवर्तन बहुपदों के सात वर्गों का प्रस्ताव दिया है, जहां $L(x) = x$ और $p = 5$ है। $\mathbb{F}_{p^{2m}}$ के एक उपसमुच्चय में कुछ निम्न डिग्री समीकरणों के समाधान की संख्या का निर्धारण हमारे निर्माण में एक महत्वपूर्ण भूमिका निभाता है।

इसके अलावा, R पर क्रमपरिवर्तन बहुपदों के क्रिप्टोग्राफ़ी और कोडिंग सिद्धांत में कई अनुप्रयोग होते हैं, ज्यादातर तब जब R एक क्षेत्र होता है। क्रमपरिवर्तन बहुपद के लिए कुछ अध्ययन अवशेष वर्ग के वलय पर है। लेकिन स्वेच्छित विनिमेय वलय के लिए तस्वीर इतनी स्पष्ट नहीं है। इस शोध प्रबंध में हमने परिमित समूह वलय पर क्रमपरिवर्तन बहुपद का भी अध्ययन किया है और समूह वलय $\mathbb{F}_p\ C_{p^n}$ (प्रमेय 6.2.1) पर क्रमपरिवर्तन बहुपद का एक वर्ग दिया है।

Contents

List of Symbols

$\mathbb{N}$	the set of natural numbers
$\mathbb{Z}$	the set of integers
p	a prime
q	a prime power
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$a \equiv b \mod n$	a congruent to b modulo n
$a \not\equiv b \mod n$	a not congruent to b modulo n
$\forall\, x$	for all x
$\lvert S \rvert$	number of elements of a finite set S
$x \in X$	x belongs to X
$x \notin X$	x does not belong to X
$A \subseteq S$	A is a subset of S
$A \nsubseteq S$	A is not a subset of S
$\gcd(a, b)$	the greatest common divisor of a and b
$\phi(n)$	Euler's phi function of n
$=$	is equal to
$\neq$	is not equal to
$\mathbb{F}_q$	finite field with q elements
$\mathbb{F}_q^*$	the multiplicative group of non zero elements of $\mathbb{F}_q$
$\mathbb{F}_q[x]$	the polynomial ring over $\mathbb{F}_q$
$Tr_1^m(\alpha)$	the trace of $\alpha \in \mathbb{F}_{q^m}$ over $\mathbb{F}_q$