# CERTAIN SPECIAL PRIMITIVE ELEMENTS IN FINITE FIELDS

SONIYA TAKSHAK


DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI

FEBRUARY 2025

# CERTAIN SPECIAL PRIMITIVE ELEMENTS IN FINITE FIELDS

by

SONIYA TAKSHAK

Department of Mathematics

Submitted

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

to the


INDIAN INSTITUTE OF TECHNOLOGY DELHI

FEBRUARY 2025

**Dedicated to**

**My Family and Friends**

# Certificate

This is to certify that the thesis entitled **"Certain special primitive elements in finite fields"** submitted by **"Soniya Takshak"** 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 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.

New Delhi
February 2025

**Prof. R. K. Sharma**
**Professor**
**Department of Mathematics**
**Indian Institute of Technology Delhi**
**New Delhi 110016**

**Prof. Ritumoni Sarma**
**Professor**
**Department of Mathematics**
**Indian Institute of Technology Delhi**
**New Delhi 110016**

# Acknowledgments

*It gives me immense pleasure to pay my gratitude to all those who have supported me throughout my Ph.D. in any form. First and foremost, my sincere appreciation goes to my thesis advisor Prof. R. K. Sharma for his constant guidance, encouragement, and motivation. He always enlightened me with his knowledge and valuable suggestions in my research work. I appreciate his positive concern and his moral support during my research struggles. My gratitude extends to my co-supervisor Prof. Ritumoni Sarma for his guidance, support, and encouragement.*

*I would like to extend my gratitude to my Student Research Committee members Prof. Aparna Mehra, Prof. Amit Priyadarshi, and Prof. Gurmail Singh Benipal for their guidance, suggestions, and support all the time. I am thankful to the faculty members and staff of the Department of Mathematics, IIT Delhi, for their support. I want to thank IIT Delhi authorities for providing me with the necessary facilities to complete my Ph.D. thesis. I am grateful to CSIR (Council of Scientific & Industrial Research) for providing me research fellowship and contingency grant.*

*My sincere thanks go to my seniors and co-authors Dr. Ambrish Awasthi and Dr. Hariom Sharma for their valuable time, suggestions, cooperation, and support in my research work. A special thanks to my senior Dr. Abhay Chaturvedi for being so patient in helping me whenever needed. I want to thank Dr. Anju Gupta and Dr. Meenu Khatkar for their guidance and affection.*

*I would like to give my heartiest appreciation to my friend Pooja Gahlyan for her love and support in every situation. Even I am thankful to my Ph.D. for introducing me to such a nice person in the form of a friend. My appreciation is also extended to my other friends and fellow lab mates, Archna, Surbhi, Raksha, Dhiraj, Abhishek, Nitin, Neha, Mohit, Astha, Gyanendra, Kanupriya, Diksha, Lalit, Naveen, Arvish, Shweta, Satyam, Ridip, Bhavna, Sonika, for creating a joyful environment around me and made my Ph.D. journey memorable.*

*My greatest appreciation goes to my family for their unconditional love, support, blessings, encouragement, and motivation. Words are not enough to express my love and respect for my parents for their silent sacrifices. I would like*

*to convey my heartfelt gratitude to my elder brother Dhara Singh for his constant support and unwavering belief in me. I want to thank my husband Dr. Vickey Nandal for being my rock during the most challenging times. His presence has been invaluable in the later times of my PhD thesis. Last but not least, I want to thank almighty God for giving me the strength and opportunity to pursue my research work.*

*February 2025* *Soniya Takshak*

# Abstract

In this thesis, we obtain a sufficient condition for the existence of a primitive normal pair $(\alpha, f(\alpha))$ over $\mathbb{F}_{q^n}$, where $f(x)$ is a non-exceptional rational function over $\mathbb{F}_{q^n}$ of degree sum $m$. Additionally, for rational functions of degree sum 4, we prove that there are only 37 and 16 exceptional values of $(q, n)$ for $q = 2^k$ and $q = 3^k$ respectively.

Next, we provide a sufficient condition for the existence of primitive normal pair $(\alpha, f(\alpha))$ over $\mathbb{F}_{q^n}$ with norm and trace of $\alpha$ to be prescribed in $\mathbb{F}_q$, where $f(x) \in \mathbb{F}_{q^n}(x)$ is a rational function of degree sum $m$. Particularly, we investigate the rational functions of degree sum 4 over $\mathbb{F}_{q^n}$, where $q = 11^k$ and demonstrate that there are only 3 exceptional pairs $(q, n), n \geq 7$ for which such kind of primitive normal pair may not exist. In general, we showed that such elements always exist except for finitely many choices of $(q, n)$.

Further, we extend our work to the existence of primitive normal triple $(\alpha, \beta, f(\alpha, \beta))$ over $\mathbb{F}_{q^n}$, where $f(x, y) = ax^2 + bxy + cy^2 \in \mathbb{F}_{q^n}[x], b^2 \neq 4ac$. Next, we generalize this result for the existence of $r$-primitive $k$-normal triple over $\mathbb{F}_{q^n}$ and discuss the existence of 2-primitive 1-normal element $\alpha$ and 2-primitive element $\beta$ in $\mathbb{F}_{q^n}$ such that $f(\alpha, \beta)$ is also 2-primitive for $q = 3^t$, where $t$ is a positive integer.

Next, we generalize our work on the existence of primitive triples by defining primarily exceptional rational functions in $n$ indeterminates. We discussed the existence of triples $(\alpha, \beta, f(\alpha, \beta))$ over $\mathbb{F}_q$, where $\alpha, \beta$ are primitive and $f(\alpha, \beta)$ is an $r$-primitive element of $\mathbb{F}_q$. In particular, this implies the existence of $\mathbb{F}_q$-primitive points on the surfaces of the form $z^r = f(x, y)$, where $r \mid q - 1$. As an example, we applied our results to the unit sphere over $\mathbb{F}_q$.

Next work in the thesis deals with primitive polynomials. Primitive polynomials have their

applications in stream cipher cryptosystems. These cryptosystems use linear feedback shift registers (LFSRs) to generate their secret keys. There are different kinds of key-stream generators like filter generators, combination generators, clock-controlled generators, etc. For a combination generator, the connection polynomial is the product of connection polynomials of constituent LFSRs. The cryptographic systems using LFSRs as their components are vulnerable to correlation attacks. The attack heavily depends on the $t$-nomial multiples of the connection polynomial for small values of $t$. In this thesis, we obtain the exact number of 4-nomial and 5-nomial multiples of the product of primitive polynomials. This helps us to choose a more suitable connection polynomial to resist the correlation attacks. Next, we disprove a conjecture by Maitra, Gupta, and Venkateswarlu.

# सार

इस शोध प्रबंध में हम सबसे पहले आदिम सामान्य युग्म $(\alpha, f(\alpha)) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ के अस्तित्व के लिए एक पर्याप्त शर्त प्राप्त करते हैं, जहाँ $f(x) \in \mathbb{F}_{q^n}(x)$ घात योग $m$ का एक गैर-असाधारण परिमेय फलन है। इसके अतिरिक्त, घात योग 4 वाले परिमेय फलनो के लिए हम यह प्रमाणित करते हैं कि $q = 2^k$ और $q = 3^k$ के लिए क्रमशः केवल 37 और 16 असाधारण मानों को छोड़कर $(q, n)$ के सभी मान हमारी पर्याप्त शर्त को संतुष्ट करते हैं।

इसके बाद, हम आदिम सामान्य युग्म $(\alpha, f(\alpha)) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ के अस्तित्व के लिए एक पर्याप्त शर्त प्रदान करते हैं, जहाँ $f(x) \in \mathbb{F}_{q^n}(x)$ एक घात योग $m$ का परिमेय फलन है एवं $\alpha$ के नॉर्म और ट्रेस को $\mathbb{F}_q$ में निर्धारित किया जाता है। विशेष रूप से, हम $\mathbb{F}_{q^n}$ के ऊपर घात योग 4 वाले परिमेय फलनो का अध्ययन करते हैं, जहाँ $q = 11^k$ है। इसके साथ ही हम यह प्रदर्शित करते हैं कि $(q, n)$ के $n \geq 7$ के लिए केवल 3 असाधारण युग्म हैं जिनके लिए इस प्रकार का आदिम सामान्य युग्म अस्तित्व में होना निश्चित नहीं है। सामान्य रूप से, हमने दिखाया कि इस प्रकार के तत्व हमेशा अस्तित्व में रहते हैं, केवल कुछ निश्चित $(q, n)$ के मानों के अलावा।

तत्पश्चात, हम अपने कार्य का विस्तार करते हुए $\mathbb{F}_{q^n}$ के ऊपर आदिम सामान्य त्रियुग्म $(\alpha, \beta, f(\alpha, \beta))$ के अस्तित्व की चर्चा करते हैं, जहाँ $f(x, y) = ax^2 + bxy + cy^2 \in \mathbb{F}_{q^n}[x]$, $b^2 \neq 4ac$ होता है। फिर हम $r-$ आदिम $k-$ सामान्य ट्रिपल के अस्तित्व के लिए इस परिणाम का सामान्यीकरण करते हैं और $\mathbb{F}_{3^t}$ में $2-$ आदिम $1-$ सामान्य तत्व $\alpha$ और $2-$ आदिम तत्व $\beta$ के अस्तित्व पर चर्चा करते हैं, जहाँ $f(\alpha, \beta)$ भी $2-$ आदिम हो।

इसके बाद, हम असाधारण परिमेय फलनो को $n-$आयाम में व्यापक रुप से परिभाषित करते हैं। हम त्रियुग्म $(\alpha, \beta, f(\alpha, \beta)) \in \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q$ के अस्तित्व पर चर्चा करते है, जहाँ $\alpha, \beta$ क्षेत्र $\mathbb{F}_q$ में आदिम तत्व हैं और $f(\alpha, \beta)$ क्षेत्र $\mathbb{F}_q$ में एक $r-$ आदिम तत्व है। विशेष रूप से हम $r \mid q - 1$ के लिए $z^r = f(x, y)$ प्रकार की सतहों पर $\mathbb{F}_q$ - आदिम बिंदुओं का अस्तित्व प्रदर्शित करते हैं। एक उदाहरण के रूप में, हमने परिमित क्षेत्र $\mathbb{F}_q$ पर परिभाषित इकाई त्रिज्या के गोले पर अपने परिणामों को लागू किया।

शोध प्रबंध के अगले भाग में आदिम बहुपदों पर कार्य किया गया है। आदिम बहुपदों का उपयोग स्ट्रीम साइफर क्रिप्टोसिस्टमो में होता है। ये क्रिप्टोसिस्टम अपनी गुप्त कुंजी उत्पन्न करने के लिए रैखिक फीडबैक शिफ्ट रजिस्टर्स (LFSRs) का उपयोग करते हैं। कुंजी-धारा उत्पन्न करने वाले विभिन्न प्रकार के जनरेटरों का उपयोग किया जाता है जैसे फिल्टर जनरेटर, संयोजन जनरेटर, घड़ी-नियंत्रित जनरेटर, आदि। संयोजन जनरेटर के लिए, कनेक्शन बहुपद घटक LFSRs के कनेक्शन बहुपदों का गुणन होता है। LFSRs का उपयोग करने वाले क्रिप्टोग्राफिक सिस्टम कोरिलेशन अटैक के प्रति संवेदनशील होते हैं। ये अटैक $t$ के छोटे मानों के लिए कनेक्शन बहुपद के $t-$नॉमियल गुणकों पर मुख्य रूप से निर्भर करते हैं। इस शोध प्रबंध में, हम आदिम बहुपदों के गुणन के $4-$नॉमियल और $5-$नॉमियल गुणकों की सटीक संख्या प्राप्त करते हैं। यह हमें कोरिलेशन अटैक का प्रतिरोध करने के लिए अधिक उपयुक्त कनेक्शन बहुपद चुनने में मदद करता है। इसके बाद, हम मैत्रा, गुप्ता,और वेंकटेश्वरलू द्वारा दी गई एक परिकल्पना को खारिज करते हैं।

# Contents

# List of Symbols

| Symbol | Meaning |
|---|---|
| $\mathbb{N}$ | the set of natural numbers |
| $q$ | a prime power |
| $\mathbb{Z}$ | the set of integers |
| $\forall\ x$ | for all $x$ |
| $a \mid b$ | $a$ divides $b$ |
| $a \nmid b$ | $a$ does not divides $b$ |
| $x \in X$ | $x$ is a member of $X$ |
| $x \notin X$ | $x$ is not a member of $X$ |
| $\lvert X \rvert$ | the cardinality of a set $X$ |
| $A \subseteq X$ | $A$ is a subset of $X$ |
| $A \nsubseteq X$ | $A$ is not a subset of $X$ |
| $\gcd(a, b)$ | the greatest comman divisor of $a$ and $b$ |
| $=$ | 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 $\mathbb{F}_q$ |

| | |
|---|---|
| $\mathbb{F}_{q^n}$ | $n$ degree extension of $\mathbb{F}_q$ |
| $\mathbb{F}$ | the algebraic closure of $\mathbb{F}_p$ |
| $\phi(n)$ | Euler's phi function of $n$ |
| $\omega(k)$ | number of distinct prime divisors of a positive integer $k$ |
| $\Omega_q(g)$ | number of distinct monic irreducible divisors of $g$ |
| $W(k)$ | number of square free divisors of a positive integer $k$ |
| $W(f(x))$ | number of square free divisors of $f(x)$ over $\mathbb{F}_q$ |
| $A \times B$ | the cartesian product of $A$ and $B$ |