# ON EXISTENCE OF SOME SPECIAL ELEMENTS OVER FINITE FIELDS

HARIOM

**DEPARTMENT OF MATHEMATICS**

**INDIAN INSTITUTE OF TECHNOLOGY DELHI**

**MAY 2021**

**ON EXISTENCE OF SOME SPECIAL ELEMENTS OVER FINITE FIELDS**

by
**HARIOM**

**Department of Mathematics**

**Submitted**

**in fulfillment of the requirements of the degree of Doctor of Philosphy**

**to the**

**Indian Institute of Technology Delhi**

**May 2021**

Dedicated to
My Family

# Certificate

This is to certify that the thesis entitled **"On Existence of Some Special Elements over Finite Fields"** submitted by **"Mr. Hariom"** 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 him 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
May 2021

# Acknowledgements

*It gives me great pleasure to express my sincere gratitude to all those who have supported me throughout the course of completing my Ph. D. thesis. First and foremost, I would like to thank almighty God for giving me strength, ability and opportunity to undertake this research work and complete it successfully.*

*I would like to extend my deepest gratitude to my supervisor, Prof. R. K. Sharma, for his constant encouragement, patient guidance, ardent dedication to perfection and useful suggestions during the planning and development of this research work. I would like to express my sincere gratitude to Prof. Aparna mehra for sparing her valuable time whenever I approached her for the suggestions.*

*I would like to give special thanks to my SRC (Student Research Committee) member Prof. Ritumoni Sarma, Prof. Amit Priyadarshi and Prof. Arun Kumar for their valuable time, suggestions, coopration and support during all the time of my research work. I am greatly indebted to all faculty members of Department of Mathematics, IIT Delhi, for their co-operation and support. Many thanks to MHRD (currently MoE) and IIT Delhi authorities for providing me the research fellowship and necessary facilities till then I require during the PhD program.*

*I appreciate all my seniors for making me comfortable in the department and motivating in the initial days of my research. I am highly indebted to Dr. Anju Gupta for her support whenever I approached her for the same. I would like to give my heartily thanks to my friends Navneet Kumar Yadav* *and Sandeep Malik for their unconditional love and support. A discussion with them always seems like a discussion with my elder brothers. I am highly thankful to my seniors, colleagues and friends, Anuj, Abhay, Dileep, Lipsy, Ruchika, Manoj, Rohit, Deepak, Vaibhav, Archna, for encouraging me and creating joyful environment in this duration. 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 cannot express my love and gratitude to my family who have always supported and encouraged me. All my achievements are outcomes of the silent sacrifice and patience of my parents. Finally, I would like to thank my friends Deepak Kumar, Kezia Saini and Harpal Singh for their encouragement and never ending support.*

*New Delhi* *Hariom*
*May 2021*

# Abstract

Let $\mathbb{F}_{q^m}$ be an extension of degree $m$ of the finite field $\mathbb{F}_q$. An element $\alpha \in \mathbb{F}_{q^m}$ is primitive if and only if it the generator of $\mathbb{F}_{q^m}^*$, the multiplicative group of non zero elements of $\mathbb{F}_{q^m}$. Further, for a rational function $f(x) \in \mathbb{F}_{q^m}(x)$, a pair $(\alpha, f(\alpha))$ is a primitive pair in $\mathbb{F}_{q^m}$ if both $\alpha$ and $f(\alpha)$ are primitive elements in $\mathbb{F}_{q^m}$. Also $\alpha \in \mathbb{F}_{q^m}$ is normal over $\mathbb{F}_q$, if the set $\{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}\}$ forms a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and trace of $\alpha$ over $\mathbb{F}_q$, denoted by $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$, is given by $\alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}$. This thesis is devoted to the study of primitive pairs, primitive pairs with prescribed traces and primitive normal pairs with one prescribed trace over finite fields.

In this thesis, we obtain a sufficient condition for the existence of primitive pair $(\alpha, f(\alpha))$ in $\mathbb{F}_q$ for non exceptional rational functions. Here, we say that a rational function $f(x)$ is non exceptional if it is not of the form $f(x) = cx^j g^d(x)$, where $j$ is any integer (positive, negative or zero), $d > 1$ divides $q-1$ and $c \in \mathbb{F}_q^*$, for any rational function $g(x) \in \mathbb{F}_q(x)$. Using that condition along with the sieving criterion for rational functions of degree sum 2, we conjectured the existence of primitive pairs in $\mathbb{F}_q$ whenever $q > 331$.

Also, for the rational functions of the form $f = f_1/f_2$, where $f_1$ and $f_2$ are co-prime irreducible polynomials over $\mathbb{F}_{q^m}$, we proved the existence of primitive pair $(\alpha, f(\alpha))$ in $\mathbb{F}_{q^m}$ such that $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{-1})$ are prescribed in $\mathbb{F}_q$. Additionally, for rational functions of degree sum 2 and $m \geq 7$, we guarantee the existence of such pairs in $\mathbb{F}_{q^m}$ for all $(q, m)$ except for at most 64 choices.

Further, we consider all the conditions simultaneously and for non exceptional rational functions, we obtain a sufficient condition for the existence of primitive pair $(\alpha, f(\alpha))$ in $\mathbb{F}_{q^m}$ such that $\alpha$ is normal over $\mathbb{F}_q$ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{-1})$ is prescribed in $\mathbb{F}_q$. We further improve this condition by proving an extension of the sieving result due to Cohen and Anju [13] for our case. Using the sufficient condition and sieving criterion for rational functions of degree sum 2, finite fields of characteristic 5 and $m \geq 3$, we proved the existence of such pairs in $\mathbb{F}_{q^m}$ except for at most 20 values of $(q, m)$.

# सारांश


मान लीजिए कि $\mathbb{F}_{q^m}$, परिमित फील्ड $\mathbb{F}_q$का डिग्री $m$ का एक एक्सटेंसन है| $\mathbb{F}_{q^m}$ का एक तत्व $\alpha$ प्रीमिटिव होगा यदि और केवल यदि वह गैर शून्य तत्वों के समूह $\mathbb{F}_{q^m}^*$का जनक है| किसी परिमेय फलन $f(x) \in \mathbb{F}_{q^m}(x)$ के लिए, एक जोड़ा $(\alpha, f(\alpha)$, $\mathbb{F}_{q^m}$ में प्रीमिटिव जोड़ा होगा यदि $\alpha$ और $f(\alpha)$ दोनों $\mathbb{F}_{q^m}$ के प्रीमिटिव तत्व हैं| साथ ही $\alpha \in \mathbb{F}_{q^m}$, $\mathbb{F}_q$ पर नॉर्मल होगा यदि समुच्चय $\{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}\}$, $\mathbb{F}_{q^m}$ का $\mathbb{F}_q$ पर एक आधार बनाता है तथा $\mathbb{F}_q$ पर $\alpha$ की ट्रैस को $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ से निरूपित किया जाता है , जिसको $\alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}$ से परिकिलित किया जाता है | यह शोध प्रबंध परिमित फील्ड मे प्रीमिटिव जोड़े, निर्धारित ट्रैस के साथ प्रीमिटिव जोड़े तथा एक निर्धारित ट्रैस के साथ प्रिमिटिव नॉर्मल जोड़े के अध्ययन के लिए समर्पित है|

इस शोध प्रबंध मे हमने गैर असाधारण परिमेय फलन के लिए $\mathbb{F}_q$ मे प्रीमिटिव जोड़ा $(\alpha, f(\alpha))$ के असितत्व के लिए पर्याप्त शर्त प्राप्त की| यहाँ, परिमेय फलन $f(x)$ गैर असाधारण होगा यदि वह $f(x) = cx^j g^d(x)$ रूप का न हो, जहां $j$ कोई भी पूर्णांक (धनात्मक, ऋणात्मक या शून्य ), $d(> 1)|q-1$, $c \in \mathbb{F}_q^*$ तथा $g(x) \in \mathbb{F}_q(x)$ कोई भी परिमेय फलन है| घात योग $2$ के परिमेय फलनों के लिए इस पर्याप्त शर्त को सीवींग मापदंड के साथ प्रयोग करके, हमने $\mathbb{F}_q$ मे, जब भी $q > 331$ हो, प्रीमिटिव जोड़ों के असितत्व का अनुमान लगाया|

साथ ही, $f = f_1/f_2$ प्रकार के परिमेय फलनों के लिए, जहां $f_1, f_2$, $\mathbb{F}_{q^m}$ पर सह अभाज्य अलघुयकरणीय बहुपद हैं, हमने $\mathbb{F}_{q^m}$ में प्रिमिटिव जोड़े $(\alpha, f(\alpha))$ के असितत्व को सिद्ध किया जहां $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ और $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{-1})$, $\mathbb{F}_q$ में निर्धारित है| इसके साथ ही, घात योग $2$ के परिमेय फलनों और $m \geq 7$ के लिए, हम $(q, m)$ के ज्यादा से ज्यादा $64$ विकल्पों के सिवाय, सभी $\mathbb{F}_{q^m}$ मे इस प्रकार के जोड़ों के अस्तित्व की प्रत्याभूति देते हैं|

आगे, हमने सभी शर्तों को एक साथ लिया और गैर असाधारण परिमेय फलनों के लिए, हमने $\mathbb{F}_{q^m}$ में प्रिमिटिव जोड़े $(\alpha, f(\alpha))$ के अस्तित्व के लिए एक पर्याप्त शर्त प्राप्त की जहां $\alpha$, $\mathbb{F}_q$ पर नॉर्मल हो तथा $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{-1})$, $\mathbb{F}_q$ मे निर्धारित हो| हमने Cohen और Anju[13] के सीवींग

परिणाम को अपने मामले मे आगे बढ़ाते हुए इस पर्याप्त शर्त को सुधारा| घात योग $2$ के परिमेय फलनों, अभिलक्षण 5 के परिमित फील्ड तथा $m \geq 3$ के लिए पर्याप्त शर्त और सीवींग मापदंड का इस्तेमाल करते हुए, हमने $(q, m)$ के ज्यादा से ज्यादा $20$ मान के सिवाय, $\mathbb{F}_{q^m}$ मे इस प्रकार के प्रिमिटिव जोड़ों के अस्तित्व को सिद्ध किया|

# Contents

# List of Symbols

| | |
|---|---|
| $\mathbb{N}$ | the set of natural numbers |
| $\mathbb{Z}$ | the set of integers |
| $q$ | a prime power |
| $a\|b$ | $a$ divides $b$ |
| $a \nmid b$ | $a$ does not divide $b$ |
| $\forall\ x$ | for all $x$ |
| $\|S\|$ | 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 comman 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 $\mathbb{F}_q$ |
| $\omega(k)$ | number of distinct prime divisors of a positive integer $k$ |
| $W(k)$ | number of square free divisors of a positive integer $k$ i.e., $W(k) = 2^{\omega(k)}$ |
| $\Omega_q(f(x))$ | number of distinct monic irreducible divisors of $f(x)$ over $\mathbb{F}_q$. |
| $W(f(x))$ | number of square free divisors of $f(x)$ over $\mathbb{F}_q$ i.e., $W(f(x)) = 2^{\Omega_q(f(x))}$ |