CONSTRUCTION OF ADDITIVE AND GALOIS LCD CODES OVER FINITE FIELDS

GYANENDRA KUMAR VERMA

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
July 2024

CONSTRUCTION OF ADDITIVE AND GALOIS LCD CODES OVER FINITE FIELDS

by

Gyanendra Kumar Verma

Department of Mathematics

Submitted

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

to the

Indian Institute of Technology Delhi

July 2024

Dedicated to my family and friends.

Certificate

This is to certify that the thesis entitled **Construction of Additive and Galois LCD Codes Over Finite Fields** submitted by **Gyanendra Kumar Verma** 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.

New Delhi
July 2024

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

Acknowledgements

I take great pleasure to express my gratitude to various people who have provided their constant support and inspiration to me in journey of my Ph.D. First of all, I would like to thanks Lord Shiva for his blessings and strength to complete this thesis. I'm grateful to my family for their love and support, which act as ongoing inspiration for me; my accomplishments are a result of their belief in me. My deepest gratitude goes to my mother and father, their affection, who continue to inspire and encourage me on this journey.

My heartfelt thanks go to my thesis supervisor, Professor R. K. Sharma, for his exceptional guidance and supervision during my Ph.D. journey. Professor Sharma not only gave me the freedom to choose my research area based on my own interests but also consistently motivated me with his unwavering support and invaluable suggestions at every stage of my research. He was always available to assist me, regardless of the time, and it was indeed a privilege to work with Prof. Sharma.

I would also like to thank my SRC (Student Research Committee) members Prof. Amit Priyadarshi, Prof. Shiv Prakash Patel and Prof. A. K. Shukla for their encouragement and thoughts from time to time. In my pre-Ph.D. course work, I learned many new mathematical concepts, I want to thank all of the instructors for their wonderful lectures. I acknowledge Council of Scientific and Industrial Research (CSIR), Govt. of India for providing the financial support throughout my Ph.D. and Department of Mathematics, IIT-Delhi for providing all the facilities required during my Ph.D.

I'd like to thank my elementary school teachers, late Mr. Radheshyam Sharma and Mr. Ramesh Kumar Mishra for sparking my interest in mathematics at an early age. I am grateful to my instructors for their great teaching and for extending my interest in mathematics during my graduation and postgraduate studies. I am thankful to Mr. Sumit Kumar for teaching me algebra and analysis after my post graduation and inspiring me for research.

I am thankful to my co-author and colleague, Astha, for having healthy discussions. I'd also want to thank my juniors/labmates for creating a good working atmosphere in the lab. I would like to express my gratitude to my friends Diskha, Khyati, Ashish, Tushar, Manuj, Himanshu, Aakash, Divay, Gurdev and Santosh for their unconditional support and creating everlasting joyful memories. I want to thank my seniors and batchmates Dr. Amit, Dr. Pooja, Dr. Soniya, Dr. Abhinay, Dr. Neha, Anshul, Abhilash, Ritika and Sachin. Finally, I'd like to thank everyone whose names I failed to add who assisted me, deliberately or inadvertently, during my Ph.D.

New Delhi Gyanendra Kumar Verma

July 2024

Abstract

Coding theory is primarily concerned with the encoding and decoding of information so that the receiver receives error-free information even when the information is transmitted through a noisy channel. As finite fields and rings are utilized as code alphabets, mathematical theories relating to finite fields and rings are important in coding theory. For practical applications, we need codes that provide efficient encoding and decoding methodologies along with easy implementation. Linear (additive) and cyclic codes are classes of codes that are suitable for practical purposes due to their algebraic structure. This thesis mainly focuses on the construction of good additive (cyclic) codes and Galois linear complementary dual (LCD) codes over finite fields and a finite chain ring.

We present a method for constructing many Hermitian LCD codes from a given Hermitian LCD code. We provide several methods that utilize either a given $[n, k, d]$ linear code or a given $[n, k, d]$ Galois LCD code to construct new Galois LCD codes with different parameters. Using these construction methods, we obtain several new $[n, k, d]$ ternary LCD codes with better parameters for $26 \leq n \leq 40$ and $21 \leq k \leq 30$. Additionally, we construct optimal 2-Galois LCD codes over the field $\mathbb{F}_{2^3}$ for code length $1 \leq n \leq 15$. We also discuss linear complementary dual codes with respect to the σ-inner product and obtain results similar to the Euclidean inner product.

Next, we investigate the additive complementary dual (ACD) codes over finite fields $\mathbb{F}_{q^2}$, where q is a prime power for the trace inner products. First, we associate an additive code with a matrix known as a generator matrix. Subsequently, we characterize ACD codes with respect to the trace Hermitian and the trace Euclidean inner products in terms of generator matrices. We also construct ACD codes over $\mathbb{F}_{q^2}$ from linear codes over $\mathbb{F}_q$. Furthermore, we provide techniques for constructing ACD codes with different parameters from a given ACD code over $\mathbb{F}_{q^2}$. Using these methods, we produce several trace Euclidean and trace Hermitian

ACD codes with better parameters than linear codes over $\mathbb{F}_9$ and $\mathbb{F}_4$. We also explore additive cyclic codes over $\mathbb{F}_{q^2}$, where q is an odd prime power. In this thesis, we obtain the algebraic structure of additive cyclic codes and determine the dual of a class of additive cyclic codes over $\mathbb{F}_{q^2}$ with respect to trace inner products. Moreover, we construct some examples of additive cyclic codes over $\mathbb{F}_9$ with better distance as compared to linear codes of the same length and size. Additionally, we characterize the subfield subcodes and the trace codes of additive cyclic codes.

In continuation, we study additive cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$, where $u^2 = 0$ and obtain generator polynomials for these codes. Further, we observe that additive cyclic codes over $\mathbb{F}_4+u\mathbb{F}_4$ can be expressed as a direct sum of additive cyclic and u times additive cyclic code over $\mathbb{F}_4$. We provide necessary and sufficient conditions for additive codes to be self-orthogonal and self-dual codes over $\mathbb{F}_4 + u\mathbb{F}_4$. We show that we can construct self-orthogonal codes over $\mathbb{F}_4$ and $\mathbb{F}_2$ via Gray maps with respect to the Symplectic inner product. Additive self-orthogonal codes are useful in the construction of quantum codes.

सार

कोडिंग सिद्धांत मुख्य रूप से सूचना के एन्कोडिंग और डिकोडिंग से संबंधित है, इस तरह कि जब सूचना एक नॉइज़ी चैनल के माध्यम से प्रसारित होने पर भी प्राप्तकर्ता त्रुटि मुक्त जानकारी प्राप्त करता है। चूंकि फाइनाइट फील्ड्स और रिंगस का उपयोग कोड वर्णमाला के रूप में किया जाता है, फाइनाइट फील्ड्स और रिंगस से संबंधित गणितीय सिद्धांत कोडिंग सिद्धांत में महत्वपूर्ण हैं। व्यावहारिक अनुप्रयोगों के लिए, हमें ऐसे कोड की आवश्यकता होती है जो कुशल एन्कोडिंग और डिकोडिंग पद्धति प्रदान करने के साथ उनका कार्यान्वयन भी आसान हो। रैखिक (योजक) और चक्रीय कोडस, कोड के वर्ग हैं जो उनकी बीजगणितीय संरचना के कारण व्यावहारिक उद्देश्यों के लिए उपयुक्त हैं। यह थीसिस मुख्य रूप से फाइनाइट फील्ड्स और एक फाइनाइट चैन रिंग पर अच्छे योजक (चक्रीय) कोडस और गैल्वा लिनीअर कॉम्पलेमेन्टरी डुअल (LCD) कोड का निर्माण पर केंद्रित है।

हम किसी दिए गए हर्मिटियन एलसीडी कोड से कई हर्मिटियन एलसीडी कोड बनाने के लिए एक विधि प्रस्तुत करते हैं। हम कई विधियाँ प्रदान करते हैं जो दिए गए एक $[n, k, d]$ रैखिक कोड या एक $[n, k, d]$ गैल्वा एलसीडी कोड का उपयोग करके विभिन्न मापदंडों के साथ नए गैल्वा एलसीडी कोड बनाता है । इन निर्माण विधियों का उपयोग करके, हम $26 \leq n \leq 40$, और $21 \leq k \leq 30$ के लिए बेहतर मापदंडों के साथ कई नए $[n,k,d]$ त्रिक (टर्नरी) एलसीडी कोड प्राप्त करते हैं। इसके अतिरिक्त, हम कोड लंबाई $1 \leq n \leq 15$ के लिए फ़ील्ड F_2^3 पर इष्टतम 2- गैल्वा एलसीडी कोड का निर्माण करते हैं। हम σ-इनर प्रोडक्ट के संबंध में लिनीअर कॉम्पलेमेन्टरी डुअल कोडों पर भी चर्चा करते हैं और यूक्लिडियन इनर प्रोडक्ट के समान परिणाम प्राप्त करते हैं।

इसके बाद, हम फाइनाइट फील्ड F_{q^2} पर ऐडिटिव कॉम्पलेमेन्टरी डुअल (ACD) कोड की ट्रेस इनर प्रोडक्ट क संबंध में जांच करते हैं, जहाँ q एक अभाज्य संख्या की घात है । सबसे पहले, हम एक एडिटिव कोड को एक मैट्रिक्स के साथ जोड़ते हैं जिसे जनरेटर मैट्रिक्स के रूप में जाना जाता है। इसके बाद, हम ट्रेस हर्मिटियन और ट्रेस यूक्लिडियन इनर प्रोडक्ट के संबंध में एसीडी कोड का वर्णन जनरेटर मैट्रिसेस के संदर्भ में बताते हैं। हम ऐडिटिव कोड ओवर F_q से F_{q^2} पर ACD कोड भी बनाते हैं। इसके अलावा, हम F_{q2} पर दिए गए ACD कोड से अलग-अलग मापदंडों के साथ ACD कोड बनाने की तकनीक प्रदान करते हैं। इन विधियों का उपयोग करके, हम F_9 और F_4 पर रैखिक कोडों की तुलना में बेहतर मापदंडों के साथ कई ट्रेस यूक्लिडियन और ट्रेस हर्मिटियन ACD कोड बनाते करते हैं। हम F_{q2} पर ऐडिटिव चक्रीय कोडों का भी पता लगाते हैं, जहाँ q एक विषम अभाज्य की घात है। इस थीसिस में, हम F_{q2} पर ऐडिटिव चक्रीय कोडों और ऐडिटिव चक्रीय कोडों के एक वर्ग के डुअल की बीजगणितीय संरचना और ट्रेस इनर प्रोडक्ट के संबंध में प्राप्त करते हैं। इसके अलावा, हम समान मापदंड के रैखिक कोड की तुलना में बेहतर दूरी के साथ F_9 पर ऐडिटिव चक्रीय कोड के कुछ उदाहरण बनाते हैं। इसके अतिरिक्त, हम ऐडिटिव चक्रीय कोडों के सब-फील्ड और ट्रेस कोडों को भी चिह्नित करते हैं।

इसी निरंतरता में, हम $F_4 + uF_4$ पर ऐडिटिव चक्रीय कोड का अध्ययन करते हैं, जहाँ $u^2 = 0$ है और इन कोडों के लिए जनरेटर बहुपद प्राप्त करते हैं। इसके अलावा, हम देखते हैं कि F_4+uF_4 पर ऐडिटिव चक्रीय कोड को F_4 पर ऐडिटिव चक्रीय और u गुना ऐडिटिव चक्रीय कोड के प्रत्यक्ष योग के रूप में व्यक्त किया जा सकता है। हम ऐडिटिव कोडों के लिए आवश्यक और पर्याप्त शर्तें प्रदान करते हैं ताकि वे F_4+uF_4 पर सेल्फ-ऑर्थोगोनल और सेल्फ-डुअल कोड बन सकें। हम दिखाते हैं कि हम सिम्प्लेक्टिक इनर प्रोडक्ट के संबंध में ग्रे-मैप्स के माध्यम से F_4 और F_2 पर सेल्फ-ऑर्थोगोनल कोड का निर्माण कर सकते हैं। एडिटिव सेल्फ-ऑर्थोगोनल कोडस क्वान्टम कोड के निर्माण में उपयोगी होते हैं।

Contents

Certificate i

Acknowledgements iii

Abstract v

List of Figures ix

List of Tables xi

List of Symbols xiii

List of Abbreviations xv

1 Introduction and Basic Concepts 1

1.1 A brief introduction to coding theory 1

1.2 Basic definitions and Notations 3

1.3 Motivation of the thesis 10

1.4 Organization of the thesis 14

2 Construction of Galois LCD Codes Over Finite Fields 15

2.1 Construction of Hermitian LCD codes 18

2.1.1 Some properties of the construction method 20

2.2 Construction of Galois LCD codes 22

2.2.1 New ternary LCD codes 26

2.2.2 2-Galois LCD codes over $\mathbb{F}_{2^3}$ 28

2.3 σ-LCD Codes 28

2.4 Conclusion 31

3 Additive Complementary Dual Codes over $\mathbb{F}_{q^2}$ 35

3.1 Trace Hermitian ACD Codes 37

3.2 Trace Euclidean ACD Codes 42

3.3 Construction of ACD codes 45

3.4 Conclusion 50

4 Trace Dual of Additive Cyclic Codes Over Finite Fields 53

4.1 Generating polynomials of additive cyclic codes and their properties 56

4.2 Trace dual of additive cyclic codes 59

4.3 Subfield and Trace code 65

4.4 Conclusion 66

5 On Additive Cyclic Codes Over a Finite Chain Ring 69

5.1 Additive cyclic code over R 71

5.2 Image of additive cyclic code under Gray maps 73

5.3 Conclusion 77

6 Conclusion and Future Directions 79

References 81

List of Publications 87

Curriculum Vitae 89

List of Figures

1.1 Without channel coding 2
1.2 With channel coding 3

List of Tables

2.1 New ternary LCD codes with better parameters 32

2.2 Bounds on minimum distance on ternary LCD codes 33

2.3 Bounds on minimum distance of 2-Galois LCD codes over $\mathbb{F}_{2^3}$ 33

3.1 Trace Euclidean ACD codes over the finite field $\mathbb{F}_9$ constructed using Theorem 3.3.2, where $w^2 + 1 = 0$. 50

3.2 Trace Hermitian ACD codes over the finite field $\mathbb{F}_9$ using Theorem 3.3.1 where $w^2 + 1 = 0$. 51

4.1 Some examples of additive cyclic codes over $\mathbb{F}_9$. 67

5.1 Gray image and Lee weight of elements of R 78

List of Symbols

$\mathbb{Z}_m$	Set of integers modulo m
$\mathbb{F}_q$	Finite field of order q
C	A code
$C^{\perp}$ or $C^{\perp_E}$	Euclidean dual of a code C
$C^{\perp_H}, C^{\perp_l}$	Hermitian dual and Galois of a code C, respectively
$C^{\perp_{TrE}}, C^{\perp_{TrH}}$	Trace Euclidean dual and trace Hermitian dual of a code C, respectively
$w(\boldsymbol{z}), w_L(\boldsymbol{z})$	Hamming weight and Lee weight of a vector $\boldsymbol{z}$, respectively
d	Distance of a code C
G	Generator matrix for a code C
Tr	Trace map
$\overline{b}$	Conjugate of an element $b \in \mathbb{F}_{q^2}$
$\in$	Belongs to
$\subseteq$	Subset
$\forall$	For all
$\mathbb{F}_q[x]$	Ring of polynomial over $\mathbb{F}_q$ in indeterminate x
$\frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle}$	Quotient ring in $\mathbb{F}_q[x]$ modulo (x^n-1)
$deg\ p(x)$	Degree of the polynomial $p(x)$
$dim_{\mathbb{F}_p}(C)$	Dimension of C as a vector space over the field $\mathbb{F}_p$

List of Abbreviations

LCD	Linear complementary dual
ACD	Additive complementary dual
$ACCD$	Additive cyclic complementary dual
$ELCD$	Euclidean linear complementary dual
$HLCD$	Hermitian linear complementary dual
$GLCD$	Galois linear complementary dual
MDS	Maximum distance separable
$BKLC$	Best known linear code