CONSTRUCTION OF LINEAR CODES WITH NICE PARAMETERS

VIDYA SAGAR

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
NOVEMBER 2023

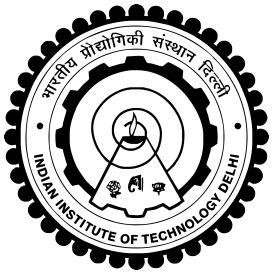
Construction of Linear Codes with Nice Parameters

by

Vidya Sagar

Department of Mathematics

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



Indian Institute of Technology Delhi
November 2023

Dedicated to

My Supervisor

and

My Family

Certificate

This is to certify that the thesis entitled "**Construction of Linear Codes with Nice Parameters**" submitted by **Mr. Vidya Sagar** 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
November 2023

Dr. Ritumoni Sarma
Associate Professor
Department of Mathematics
Indian Institute of Technology Delhi

Acknowledgments

I would like to extend my sincere gratitude to my doctoral supervisor, Prof. Ritumoni Sarma, whose expertise was invaluable in formulating the research problems and methodology. His insightful feedback pushed me to sharpen my thinking and bring my work to a higher level. With deep respect, I acknowledge his academic and emotional support through the rough road to finishing this thesis. The independence he granted me helped me grow as an independent researcher. I want to thank him for providing me with the best support during these years, which is friendship. Thus, we could discuss freely on many occasions regarding many aspects of life, which immensely helped me lead a healthy and better life. I am also thankful to him for allowing me to be a part of national and international conferences/workshops, where I learned many things. Thank you for your vital support and belief in my research abilities.

I would like to extend my appreciation to the Student Research Committee (SRC) members Prof. R. K. Sharma, Prof. Surjeet Kour, and Prof. S. D. Joshi (EE) for their valuable time and suggestions. I would also like to thank Prof. Shiv Prakash Patel for his guidance and encouragement. I am also grateful to to all the faculty members of the Department of Mathematics, IIT Delhi, for their cooperation and support.

I am deeply indebted to to Prof. Yansheng Wu (Nanjing University of Posts and Telecommunications, China) for his help and support.

The Department of Mathematics, IIT Delhi has provided the support and facilities that I needed to complete my thesis. I thank IIT Delhi for providing financial support to attend the international conferences "ALCOCRYPT 2023" (held at CIRM, Luminy, France) and "Fq15" (held at Campus Condorcet, Aubervilliers, Paris, France). I would also like to thank the International Centre for Pure and Applied Mathematics (CIMPA) and the National Centre for Mathematics (NCM) for providing

financial support to attend the CIMPA school 2022 held at Helwan University, Cairo, Egypt, and the AFS-1 2018 held at IISER Bhopal, Madhya Pradesh, India, respectively.

I acknowledge the Indian Institute of Technology Delhi for providing me the opportunity to study at this prestigious institution, providing financial assistance for my research work, and the efficient management of the official processes throughout these years.

I am grateful to all of my seniors, batchmates, and juniors for making me comfortable in the department and motivating me over the past five years. It seems 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, Jyotsna, Tanvi, Sakshi, Bhawna, Ritesh, Abhinay, Mohit, Himanshu, Anuj, Akanksha, Ankit, Raju, Aastha, Gyanendra, Praveen Manju, Shweta, Satyam, Kavin, Ritika, Abhilash, Anshul, Nitin, Abhishek, Navneet, Rattan Lal and Vikram (EE). Some special words of gratitude go to my friends who have always been a major source of support, suggestions, and motivation when things would get a bit discouraging: Saurabh Verma (IIIT Allahabad, India), Kshitij, Edgar, and Neha. Thank you, everyone, for always being there for me.

My heartfelt gratitude goes to my best friend, Mohit Pal, for his never-ending encouragement and inspiring conversations.

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 lifelong support, which sustained my interest in research and motivated me towards the successful completion of this study. I want to express my sincere gratitude to my sister Rashmi Rani and my brother Kumar Deobrat for their love, patience, belief, and understanding. I would also like to thank my friends Vikash and Vikramadity, my brother-in-law Mukesh, and my nieces Ayushi and Aaradhya.

Above all, I am grateful to the Almighty God for blessing me with strength and wisdom.

New Delhi *Vidya Sagar*
November 2023

Abstract

In a communication system, data are transmitted from a sender to a receiver via a channel. This channel is often affected by many sources of noise and interference, which may damage the data during transmission. It is not always possible to get rid of this problem by simply improving the quality of communication channel. To overcome this situation, error-correcting codes are helpful upto a great extent to detect and even correct errors that occur when data are transmitted across some noisy channel. Linear codes have been in use in communication systems and data storage in daily life. We are interested in codes with high error-correcting capacity and minimum redundancy; in other words, we want to find codes with large minimum "Hamming distance" and small "length". High minimum distance and small length are controversial goals for the optimization of codes. A linear code C is called distance optimal if there exists no linear code with higher minimum distance (than that of C) but with the same code length and the same code size (as that of C). A distance optimal code has the highest possible error-correcting capacity for a given code length and code size.

Secret sharing schemes are becoming essential nowadays; in fact, these are used heavily in electronic voting systems, cryptographic protocols, banking systems, etc. "Minimal linear codes" have interesting applications in secret sharing schemes and secure two-party computation. "LCD codes" are important linear codes due to their use in implementations against side-channel attacks and fault injection attacks. Thus, it is of great interest to construct and investigate linear codes which have many applications, for instance, LCD codes, minimal codes and distance optimal codes.

In this thesis, we construct linear codes over certain finite fields and finite rings and study their algebraic structures. The non-unital rings I, E and F (notation is due to Fine [26]) are used as code alphabets. We use the mathematical object called simplicial complex in this construction. Using these linear codes, we obtain two types of binary linear codes. The first one (called subfield or subfield-like codes) is obtained with the help of certain linear functionals (for instance, the trace map) and

the other one is obtained with the help of certain isomorphisms of vector spaces (called Gray maps). The weight distributions of all these codes are computed. Most of these binary codes are few-weight minimal linear codes. With respect to the "Griesmer bound", a few classes of distance optimal codes are obtained. Sufficient conditions for these binary linear codes to be self-orthogonal are obtained. This is the first attempt to study the structure of linear codes over non-unital rings using simplicial complexes.

The hull of a linear code is the intersection of the code with its dual. We construct linear codes over finite fields using multiplicative characters of other finite fields and study their hull. We discuss certain sufficient conditions under which these are either linear complementary dual (in short, LCD) codes or linear codes with one-dimensional hull. General Gauss sums are used heavily to achieve these results. Finally, we show that if the base field is of characteristic 2, these codes are "isodual". An additive complementary dual (in short, ACD) code is a generalization (in fact, an exact analogue) of an LCD code in the class of additive codes. ACD codes are considered over the ring $\mathbb{Z}_2\mathscr{R}$, where $\mathscr{R} = \frac{\mathbb{Z}_2[u]}{\langle u^4 \rangle}$. We investigate free "self-dual codes" over $\mathscr{R}$. A condition that ensures an additive code to be an ACD code is established. Furthermore, for a separable additive code to be an ACD code, a necessary and sufficient condition is established. We consider a Gray map under which certain additive codes become binary LCD codes. We also present a few optimal (or almost optimal) binary LCD codes. Moreover, a number of weight enumerators are computed and the corresponding "MacWilliams identities" are discussed.

सार

संचार प्रणाली में, डेटा एक चैनल के माध्यम से प्रेषक से रिसीवर तक प्रेषित किया जाता है। यह चैनल अक्सर शोर और हस्तक्षेप के कई स्रोतों से प्रभावित होता है, जो ट्रांसमिशन के दौरान डेटा को नुकसान पहुंचा सकता है। केवल संचार चैनल की गुणवत्ता में सुधार करके इस समस्या से छुटकारा पाना हमेशा संभव नहीं होता है। इस स्थिति से उबरने के लिए, एरर-करेक्टिंग (त्रुटि-सुधार) करने वाले कोड किसी नॉइस (शोर) वाले चैनल में डेटा स्टोरेज होने पर होने वाली त्रुटियों का पता लगाने और उन्हें ठीक करने में काफी हद तक सहायक होते है। दैनिक जीवन में संचार प्रणालियों और डेटा स्टोरेज में लीनियर (रैखिक) कोड का उपयोग किया गया है। हम उच्च त्रुटि-सुधार क्षमता और न्यूनतम अतिरेक वाले कोड में रुचि रखते है; दूसरे शब्दों में, हम बड़े न्यूनतम "हैमिंग दूरी" और कम "लंबाई" वाले कोड ढूंढना चाहते है। कोड के ऑप्टिमाइजेशन (इष्टतमीकरण) के लिए उच्च न्यूनतम दूरी और कम लंबाई विवादास्पद लक्ष्य है। यदि समान कोड लंबाई, समान कोड आकार और उच्च न्यूनतम दूरी के साथ कोई लीनियर कोड मौजूद नहीं है, तो उस लीनियर कोड को डिस्टेंस ऑप्टीमल (दूरी इष्टतम) कहा जाता है। किसी दिए गए कोड की लंबाई और कोड आकार के लिए डिस्टेंस ऑप्टीमल कोड में उच्चतम संभावित एरर-करेक्टिंग क्षमता होती है।

सीक्रेट शेयरिंग स्कीम (गुप्त साझाकरण योजनाएँ) आजकल आवश्यक होती जा रही है; वास्तव में, इनका उपयोग इलेक्ट्रॉनिक वोटिंग सिस्टम, क्रिप्टोग्राफ़िक प्रोटोकॉल, बैंकिंग सिस्टम आदि में बहुत ज्यादा किया जाता है। मिनिमल लीनियर कोड का सीक्रेट शेयरिंग स्कीम और सुरक्षित दो-

पक्षीय गणना में दिलचस्प अनुप्रयोग है। साइड-चैनल अटैक और फाल्ट इंजेक्शन अटैक के खिलाफ कार्यान्वयन में उपयोग के कारण "एल सी डी कोड" महत्वपूर्ण लीनियर कोड है। इस प्रकार, लीनियर कोड का निर्माण और जांच करना बहुत रुचिकर है जिसमें कई अनुप्रयोग होते है, उदाहरण के लिए, एल सी डी कोड, मिनिमल कोड और डिस्टेंस ऑप्टीमल कोड।

इस थीसिस में, हम कुछ फाइनाइट फील्ड (परिमित क्षेत्रों) और फाइनाइट रिंग (परिमित वलय) पर लीनियर कोड बनाते है और उनकी बीजगणितीय संरचनाओं का अध्ययन करते है। नॉन यूनिटल रिंग (गैर-इकाई वाले वलय) I, E और F ([26]) को कोड अल्फाबेट (वर्णमाला) के रूप में उपयोग किया है। हम इस निर्माण में सिम्प्लिसिअल काम्प्लेक्स नामक गणितीय वस्तु का उपयोग करते है। इन लीनियर कोडों का उपयोग करके, हम दो प्रकार के बाइनरी लीनियर कोड प्राप्त करते है। पहला (जिसे सबफील्ड या सबफील्ड-लाइक कोड कहा जाता है) कुछ लीनियर फंक्शनल (उदाहरण के लिए, ट्रेस मैप) की मदद से प्राप्त किया जाता है और दूसरा वेक्टर स्पेस के कुछ आइसोमोर्फिज्म (जिसे ग्रे मैप कहा जाता है) की मदद से प्राप्त किया जाता है। इन सभी कोडों के वेट डिस्ट्रीब्यूशन (भार वितरण) की गणना की जाती है। इनमें से अधिकांश बाइनरी कोड कम भार वाले मिनिमल लीनियर कोड है। "ग्रिस्मर बाउंड" के संबंध में, डिस्टेंस ऑप्टीमल कोड के कुछ वर्ग प्राप्त होते है। इन बाइनरी लीनियर कोडों के सेल्फ-ऑर्थोगोनल होने के लिए पर्याप्त शर्त प्राप्त की जाती है। यह सिम्प्लिसिअल काम्प्लेक्स का उपयोग करके नॉन यूनिटल रिंगों पर लीनियर कोड की संरचना का अध्ययन करने का पहला प्रयास है।

एक लीनियर कोड का हल उसके ड्यूल के साथ कोड का इंटरसेक्शन (प्रतिच्छेदन) है। हम अन्य फाइनाइट फील्ड के मल्टिप्लिकेटिव करैक्टर का उपयोग करके फाइनाइट फील्ड पर लीनियर कोड बनाते है और उनके हल का अध्ययन करते है। हम कुछ पर्याप्त शर्तों पर चर्चा करते है जिनके तहत ये या तो लीनियर कॉम्प्लिमेंटरी ड्यूल (संक्षेप में, एल सी डी) कोड या वन-डायमेंशनल हल वाला लीनियर कोड है। इन परिणामों को प्राप्त करने के लिए सामान्य गॉस सम का काफी उपयोग किया जाता है। अंत में, हम दिखाते है कि यदि आधार फ़ील्ड करैक्टर 2 का है, तो ये कोड "आइसोडुअल" हैं। एक एडिटिव कॉम्प्लिमेंटरी ड्यूल (संक्षेप में, ए सी डी) कोड एडिटिव कोड की श्रेणी में एक एल सी डी कोड का एक सामान्यीकरण (वास्तव में, एक सटीक एनालॉग) है।

एसीडी कोड को रिंग $\mathbb{Z}_2R$ के ऊपर अध्ययन किया जाता है, जहां $R = \mathbb{Z}_2[u]/\langle u^4 \rangle$ है। हम R पर फ्री सेल्फ ड्यूल कोड की जांच करते है। एक शर्त जो यह सुनिश्चित करती है कि एक एडिटिव कोड एक ए सी डी कोड हो, स्थापित किया जाता है। इसके अलावा, एक सेपारेबल एडिटिव कोड के ए सी डी कोड होने के लिए, एक आवश्यक और पर्याप्त शर्त स्थापित की जाती है। हम एक ग्रे मैप पर विचार करते है जिसके अंतर्गत कुछ एडिटिव कोड बाइनरी एल सी डी कोड बन जाते है। हम कुछ इष्टतम (या लगभग इष्टतम) बाइनरी एल सी डी कोड भी प्रस्तुत करते है। इसके अलावा, कई वेट एनुमेरेटर की गणना और संबंधित "मैकविलियम्स आइडेंटिटी" पर चर्चा की जाती है।

Contents

List of Tables

List of Symbols

Symbol	Meaning
$\mathbb{N}$	The set of natural numbers
$[m]$	The set of the first m natural numbers
Δ_L	The simplicial complex generated by the subset $L \subseteq [m]$
$\lvert L \rvert$	The cardinality of the set L
$\mathbb{Z}$	The ring of integers
$\mathbb{Z}_n$	The ring of integers modulo n
R/I	Quotient ring of R modulo I
$\mathbb{F}_q$	The finite field of order q, where q is some prime power
$\lceil \cdot \rceil$	The ceiling function
$\lfloor \cdot \rfloor$	The floor function
wt_H	The Hamming weight
d_H	The Hamming distance
wt_{Lee}	The Lee weight
d_{Lee}	The Lee distance
$\mathcal{O}_K$	The ring of algebraic integer in K, where K is a number field
$Hull(C)$	The hull of a linear code C
$\delta_{i,j}$	The Kronecker delta function