SMALL DIMENSIONAL HULL CODES OVER FINITE FIELDS AND FINITE NON-CHAIN RINGS

ASTHA AGRAWAL

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
July 2024

© Indian Institute of Technology Delhi (IITD), New Delhi, 2024

Small Dimensional Hull Codes Over Finite Fields And Finite Non-chain Rings

by

ASTHA AGRAWAL

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 Maharaj ji and Parents.

Certificate

This is to certify that the thesis entitled **"Small Dimensional Hull Codes Over Finite Fields and Finite Non-Chain Rings"** submitted by **Astha Agrawal** 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.

New Delhi

2024

Prof. R. K. Sharma

Professor

Department of Mathematics

Indian Institute of Technology Delhi

New Delhi 110016

Acknowledgements

I am filled with profound gratitude as I extend my heartfelt appreciation to the individuals who have pivotal roles in guiding and inspiring me throughout my PhD journey. At the forefront, I am compelled to acknowledge the boundless blessings, unwavering strength, and invaluable opportunities bestowed upon me by the Almighty. Through divine grace, I have found the fortitude to successfully navigate the path towards completing this thesis.

I am extending my sincere gratitude to my supervisor, Prof. R. K. Sharma, for their support, insightful guidance, and invaluable expertise. His consistent motivation, dedication to perfection, and invaluable suggestions at every stage of my research significantly contributed to the quality of this thesis. I appreciate the freedom that he granted me to pursue my work. Beyond academic direction, he has instilled a profound sense of confidence and commitment.

I would like to thank the members of my Student Research Committee (SRC), namely Prof. Amit Priyadarshi, Prof. Punit Sharma, and Prof. Seema Sharma, for their invaluable feedback. Their dedication to reviewing my work and offering valuable suggestions is greatly appreciated. Additionally, I extend my thanks to Prof. B. K. Dass from the University of Delhi for generously sparing time from his demanding schedule to attend my seminar for the extension of my University Grants Commission (UGC) fellowship. I acknowledge with gratitude the UGC for providing essential financial support throughout my PhD journey.

I appreciate the Indian Institute of Technology, Delhi, for granting me essential resources, library access, and facilities pivotal to my research. Special thanks to the Research Scholar Travel Award (RSTA) for enabling me to present my research work at the 'International Conference on Finite Fields and Their Applications 2023 (Fq15)' in Paris (France). The Department of Mathematics at

IIT Delhi has been an invaluable support throughout my academic journey, offering crucial intellectual discussions and seminars that enriched my research.

I am highly thankful to the individuals who have enriched my PhD experience with their camaraderie and positivity. An acknowledgement goes to my friends Raju, Gyanendra, Prachi, Sonika and Sushmita di for leaving an indelible mark on my time at IIT and making it memorable and purposeful. Allow me to extend a special thanks to my dear friend Raju for sharing all my sorrow and frustration, always believing in me, encouraging me to dream big, and pushing me every day to unlock my highest potential! His presence in my life has made a significant positive impact, and I truly appreciate it. I want to express my appreciation for my colleague and particularly my co-author, Gyanendra, for his unwavering support, both in academic and emotional aspects, throughout this journey. A big thanks goes to my lovely friend Prachi for her love and care for me over the past decade. I hold Sushmita di and Sonika's friendship in high esteem, and I am grateful for their quick bits of help. I am also thankful to my friends Abhilash, Anshul, Ritika, Sachin, Shweta, Satyam, Dr. Gurdev Anthal, Dr. Sushmita Rawat, Dr. Pooja, Soniya Ma'am, Neha Ma'am, Dr. Nitin Jaiswal, Dr. Kshitiz Pandey, and Dr. Vidya Sagar for their assistance and support.

In the end, I want to express my deepest gratitude to my family, Maharaj ji, Maa, Papa, Jiji, and Nonu, for their unwavering love, support, and understanding throughout my academic journey. Their support and understanding during this challenging phase of my life have been invaluable. Their love, encouragement, and faith in my abilities have been a continuous source of inspiration. I dedicate this thesis to them wholeheartedly.

To sum up, the successful culmination of this thesis would not have been achievable without the contributions of the individuals and institutions mentioned earlier. I extend my thanks to all who have been part of this significant milestone in my academic journey. If I unintentionally omitted anyone, please understand that your support has been deeply valued.

New Delhi *Astha Agrawal*

2024

Abstract

Algebraic Coding Theory finds crucial applications in various domains, from secure communications to quantum computing. The 'hull' of a code is essential for understanding the automorphism group of a linear code. Also, it is useful in evaluating the complexity of certain algorithms which check the permutation equivalence of two linear codes. This is particularly true when the hull's dimension is small. This thesis delves into the realm of small dimensional hull codes over finite fields and finite non-chain rings.

The thesis begins by extending the study of l-Galois Linear Complementary Dual (LCD) codes from finite chain rings to finite non-chain rings. We introduce a correspondence between l-Galois dual of linear codes over the finite non-chain ring and l-Galois dual of their component codes over finite fields. From this foundation, we construct both Euclidean and l-Galois LCD codes, ultimately revealing the equivalence of any linear code to Euclidean and l-Galois LCD codes over the finite non-chain ring. In addition, the study includes Maximum Distance Separable (MDS) codes over the non-chain ring.

Next, the focus shifts towards additive codes, as they play a pivotal role in quantum error correction and quantum computing. Additive codes, being defined over an additive group, have a broader range than linear codes, which are inherently additive. Apart from their applications in quantum computing, additive codes offer various forms of dualities using group characters. Specifically, in this thesis, the Additive Complementary Dual (ACD) codes are studied with respect to skew-symmetric dualities over the additive group of finite fields. The introduction of skew-symmetric dualities introduces a new facet. The precise count of symmetric and skew-symmetric dualities over finite fields is determined. The criteria for an additive code to be an ACD code under arbitrary dualities are unveiled, along with the necessary condition on the generator matrix for ACD codes over skew-symmetric dualities. Notably,

bounds for the highest possible minimum distance of ACD codes over skew-symmetric dualities are established. In addition, we identify some quaternary codes over non-symmetric dualities with better parameters than symmetric ones.

Further, the thesis introduces additive codes with one-rank hull, offering key insights and construction methodologies. A novel approach is developed, establishing a link between self-orthogonal elements and solutions of quadratic forms, thus setting the stage for the existence of one-rank hull codes over finite fields. The precise counting of self-orthogonal elements over finite fields, particularly focusing on odd primes, is done. The highest possible minimum distance among additive one-rank hull codes is denoted by $d_1[n,k]_{p^e,M}$. Determining the value of $d_1[n,k]_{p^e,M}$ for $k = 1,2$ with respect to any duality M over any finite field further extend the results. Finally, identifying new quaternary one-rank hull codes over non-symmetric dualities demonstrates their improved parameters compared to the symmetric dualities.

In a culmination of this exploration, the thesis introduces the study of Matrix product codes with respect to M-symplectic duality. Matrix-product code is one of the most significant class of long additive codes over finite fields. These codes are created by combining numerous comparable shorter additive codes with a defining matrix over finite fields. This study revolves around the application of Linear Algebra in analyzing Matrix product codes. Specifically exploring aspects such as the symplectic distance $d_s(C)$, the M-symplectic hull, and the rank of the M-symplectic hull for Matrix product codes. A crucial requirement for establishing a lower bound for $d_s(C)$ is ensuring that the defining matrix is 'non-singular by columns' (NSC). Additionally, we investigate scenarios where the defining matrix is quasi-symplectic, enabling us to determine the rank of the M-symplectic hull for the Matrix product code. Consequently, we demonstrate how Matrix product codes can be used to construct quantum stabilizer codes.

सार

अलजेब्रिक कोडिंग थ्योरी विभिन्न क्षेत्रों में महत्वपूर्ण अनुप्रयोग रखती है, जैसे कि सुरक्षित संचार और क्वांटम कंप्यूटिंग। एक कोड का 'हल' एक लीनियर कोड के ऑटोमोर्फिज्म समूह को समझने के लिए आवश्यक है। इसके अलावा, यह उन एल्गोरिदम की जटिलता का मूल्यांकन करने में सहायक होता है जो दो लीनियर कोड्स की परमुटेशन समतुल्यता की जांच करते हैं। यह विशेष रूप से तब सही है जब हल का आयाम छोटा हो। यह शोध प्रबंध फाइनाइट फील्ड्स और फाइनाइट नॉन-चेन रिंग्स पर छोटे आयामी हल कोड्स के क्षेत्र में अध्ययन है।

यह शोध प्रबंध फाइनाइट चेन रिंग्स से फाइनाइट नॉन-चेन रिंग्स तक l-गैल्वा लीनियर कॉम्प्लीमेंटरी ड्यूल (एलसीडी) कोड्स के अध्ययन का विस्तार करके शुरू होता है। हम फाइनाइट नॉन-चेन रिंग पर लीनियर कोड्स के l-गैल्वा ड्यूल और फाइनाइट फील्ड्स पर उनके घटक कोड्स के l-गैल्वा ड्यूल के बीच एक संगतता का परिचय देते हैं। इस आधार से, हम दोनों यूक्लिडियन और l-गैल्वा एलसीडी कोड्स का निर्माण करते हैं, और अंततः फाइनाइट नॉन-चेन रिंग पर किसी भी लीनियर कोड की यूक्लिडियन और l-गैल्वा एलसीडी कोड्स के समतुल्य होने का खुलासा करते हैं। इसके अतिरिक्त, अध्ययन में नॉन-चेन रिंग पर मैक्सिमम डिस्टेंस सेपरेबल (एमडीएस) कोड्स भी शामिल हैं।

इसके बाद, ध्यान एडिटिव कोड्स की ओर स्थानांतरित होता है, क्योंकि वे क्वांटम एरर करेक्शन और क्वांटम कंप्यूटिंग में एक महत्वपूर्ण भूमिका निभाते हैं। एडिटिव कोड्स, जो एक एडिटिव समूह पर परिभाषित होते हैं, लीनियर कोड्स की तुलना में व्यापक क्षेत्र में आते हैं, जो स्वाभाविक रूप से एडिटिव होते हैं। क्वांटम कंप्यूटिंग में उनके अनुप्रयोगों के अलावा, एडिटिव कोड्स ग्रुप कैरक्टर्स का उपयोग करके विभिन्न प्रकार की ड्यूलिटीज़ प्रदान करते हैं। विशेष रूप से, इस शोध प्रबंध में, एडिटिव कॉम्प्लीमेंटरी ड्यूल (एसीडी) कोड्स को फाइनाइट फील्ड्स के एडिटिव समूह पर स्किउ-सिमेट्रिक ड्यूलिटीज़ के संदर्भ में अध्ययन किया गया है। स्किउ-सिमेट्रिक ड्यूलिटीज़ का परिचय एक नया आयाम जोड़ता है। फाइनाइट फील्ड्स पर सिमेट्रिक और स्किउ-सिमेट्रिक ड्यूलिटीज़ की सटीक गणना निर्धारित की गई है। किसी एडिटिव कोड को आर्बिट्रेरी ड्यूलिटीज़ के तहत एसीडी कोड बनने के मानदंडों का खुलासा किया गया है, साथ ही स्किउ-सिमेट्रिक ड्यूलिटीज़ के लिए एसीडी कोड्स के जेनरेटर मैट्रिक्स पर आवश्यक शर्तें भी बताई गई हैं। विशेष रूप से स्किउ-सिमेट्रिक ड्यूलिटीज़ पर एसीडी कोड्स की सर्वोच्च संभावित न्यूनतम दूरी के लिए सीमाएं स्थापित की गई हैं। इसके अतिरिक्त, हमने नॉन-सिमेट्रिक ड्यूलिटीज़ पर कुछ क्वाटर्नरी कोड्स की पहचान की है, जिनके पैरामीटर सिमेट्रिक ड्यूलिटीज़ पर कोड्स की तुलना में बेहतर हैं।

आगे, यह शोध प्रबंध वन-रैंक हल वाले एडिटिव कोड्स को प्रस्तुत करता है, जो प्रमुख अंतर्दृष्टियाँ और निर्माण पद्धतियाँ प्रदान करता है। एक नवीन दृष्टिकोण विकसित किया गया है, जो सेल्फ-आर्थोगोनल तत्वों और क़्वाड्रेटिक फॉर्म्स के समाधानों के बीच एक संबंध स्थापित करता है, और फाइनाइट फील्ड्स पर वन-रैंक हल कोड्स के अस्तित्व के लिए मंच तैयार करता है। फाइनाइट फील्ड्स पर सेल्फ-आर्थोगोनल तत्वों की सटीक गणना की गई है, विशेष रूप से विषम

प्राइम्स पर ध्यान केंद्रित किया गया है। एडिटिव वन-रैंक हल कोड्स के बीच सर्वोच्च संभावित न्यूनतम दूरी को $d_1[n,k]_{p^e,M}$ द्वारा निरूपित किया गया है। किसी भी फाइनाइट फील्ड्स पर किसी भी ड्यूलिटीज़ के संदर्भ में $k = 1, 2,$ के लिए $d_1[n,k]_{p^e,M}$ के मूल्य को निर्धारित करना परिणामों को और विस्तारित करता है। अंत में, नॉन-सिमेट्रिक ड्यूलिटीज़ पर नए और बेहतर पैरामीटर वाले क्वाटर्नरी वन-रैंक हल कोड्स की पहचान की गयी है जो सिमेट्रिक ड्यूलिटीज़ की तुलना में अधिक प्रभावी हैं।

इस अन्वेषण के समापन में, यह शोध प्रबंध M-सिम्पलेक्टिक ड्यूलिटीज़ के संदर्भ में मैट्रिक्स प्रोडक्ट कोड्स के अध्ययन को प्रस्तुत करता है। मैट्रिक्स-प्रोडक्ट कोड्स फाइनाइट फील्ड्स पर लंबे एडिटिव कोड्स के सबसे महत्वपूर्ण वर्गों में से एक हैं। इन कोड्स को फाइनाइट फील्ड्स पर कई छोटे एडिटिव कोड्स को एक परिभाषित मैट्रिक्स के साथ जोड़कर बनाया जाता है। यह अध्ययन मैट्रिक्स प्रोडक्ट कोड्स के विश्लेषण में लीनियर एल्जेब्रा के अनुप्रयोग के इर्द-गिर्द घूमता है। विशेष रूप से, सिम्पलेक्टिक दूरी $d_s(C)$, M-सिम्पलेक्टिक हल, और M-सिम्पलेक्टिक हल की रैंक जैसे पहलुओं का अन्वेषण करता है। सिम्पलेक्टिक दूरी के लिए निम्न सीमा स्थापित करने के लिए एक महत्वपूर्ण आवश्यकता यह है कि परिभाषित मैट्रिक्स 'नॉन सिंगुलर बाई कॉलम्स (एनएससी)' हो। इसके अतिरिक्त, हम उन परिदृश्यों की जांच करते हैं जहाँ परिभाषित मैट्रिक्स क्वासी-सिम्पलेक्टिक है, जिससे हम मैट्रिक्स प्रोडक्ट कोड के लिए M-सिम्पलेक्टिक हल की रैंक निर्धारित कर सकते हैं। परिणामस्वरूप, हम प्रदर्शित करते हैं कि मैट्रिक्स प्रोडक्ट कोड्स का उपयोग क्वांटम स्टेबलाइजर कोड्स को बनाने में कैसे किया जा सकता है।

Contents

Certificate **i**

Acknowledgements **iii**

Abstract **v**

List of Symbols **xiii**

List of Tables **xv**

1 Introduction **1**

1.1 Motivation of Thesis 4

1.2 Organization of Thesis 6

2 Preliminaries **9**

2.1 Linear codes over finite fields 9

2.2 Linear codes over $\mathcal{R} = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$ 12

2.3 Additive codes over finite fields 14

2.4 Dualities over finite fields 15

2.4.1 M-symplectic duality 18

3 Galois LCD Codes Over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$ **21**

3.1 Motivation 22

3.2 l-Galois linear codes over $\mathcal{R}$ 22

3.3 Construction of Galois LCD code equivalent to linear code 26
3.4 MDS codes over $\mathcal{R}$ 30

4 ACD Codes over Skew-symmetric Dualities **33**
4.1 Motivation 34
4.2 ACD codes over arbitrary dualities 34
4.3 Skew-symmetric dualities 37
4.4 ACD codes over skew-symmetric dualities 42
4.5 Bounds of ACD codes over skew-symmetric dualities 46
4.6 Non-symmetric dualities over $\mathbb{F}_4$ 50

5 Additive One-rank Hull Codes over Finite Fields **53**
5.1 Motivation 54
5.2 Characterization of one-rank hull codes 54
5.3 Existence of one-rank hull codes 57
5.4 Constructions of small rank hull codes 61
5.5 Optimal additive codes with one-rank hull 66

6 Symplectic Dual of Matrix Product Codes **79**
6.1 Motivation 80
6.2 Characterization of M-symplectic hull of additive codes 80
6.3 Matrix product codes with respect to M-symplectic duality 84
6.3.1 Symplectic distance of Matrix product codes 85
6.3.2 M-symplectic dual of Matrix product codes 88
6.3.3 Rank of the M-symplectic hull of Matrix product codes 90
6.3.4 The Plotkin sum code 93
6.4 Application of Matrix product codes in the construction of quantum codes 96

7 Conclusions and Future Outlooks **99**
7.1 Conclusion 99
7.2 Applications 101
7.3 Future Outlooks 101

References **103**

Appendix A Generator Matrices of Quaternary ACD codes over Non-symmetric Dualities **113**

A.1 Algorithm 113

A.2 Generator matrices 115

Appendix B Generator Matrices of Quaternary One-rank Hull codes over Non-symmetric Dualities **137**

B.1 Algorithm 137

B.2 Generator matrices 138

List of Publications **159**

Curriculum Vitae **161**

List of Symbols

Symbol	Meaning
p	prime,
q	a prime power,
$\mathbb{F}_q$	finite field with q elements,
$\mathbb{F}_q^*$	the multiplicative group of non-zero elements of $\mathbb{F}_q$,
$=$	equal to,
$\neq$	not equal to,
$\exists$	there exists,
$\nexists$	there does not exists,
$\forall$	for all,
$\cup$	union,
$\cap$	intersection,
$\in$	belongs to,
$\notin$	does not belong to,
$a \mid b$	a divides b,
$a \nmid b$	a does not divide b,
$a \equiv b \mod p$	a congruent to b modulo p,
$a \not\equiv b \mod p$	a does not congruent to b modulo p,
$\emptyset$	empty set,
$\|X\|$	number of elements of a finite set X,

$A \subseteq X$	A is a subset of X,
$A \nsubseteq X$	A is not a subset of X,
$\mathcal{R}$	finite non-chian ring $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$,
$[n, k, d]$	a linear code of length n, dimension k, and minimum distance d,
(n, p^k, d)	an additive code of length n, cardinality p^k, and minimum distance d,
$((n, K, D))$	a quantum code of length n, dimension K, and minimum distance D,
$d_s(C)$	symplectic distance of a code C,
M	duality over finite fields,
$C^{\perp}$	eulidean dual of a linear code C,
$C^{\perp_l}$	l-Galois dual of a linear code C,
C^M	orthogonal code of an additive code C with respect to duality M,
C^{M_s}	orthogonal code of C with respect to M-symplectic duality,
χ_a	character of a group G corresponding to an element a,
$Hom(\mathbb{F}_q, \mathbb{C}^*)$	set of all homomorphism from $\mathbb{F}_q$ to $\mathbb{C}^*$,
ξ	the complex primitive p-th root of unity,
$\log_\xi$	the principal branch of complex logarithm to the base ξ,
$ACD_{p^e,M}[n, k]$	highest possible minimum distance among (n, p^k) ACD codes,
$d_1[n, k]_{p^e,M}$	highest possible minimum distance among (n, p^k) one-rank hull codes,
$Hull_{M_s}(C)$	hull of an additive code C with respect to M-symplectic duality,
$\lceil \cdot \rceil$	the smallest integer greater than or equal to $(\cdot)$,
$\lfloor \cdot \rfloor$	the largest integer less than or equal to $(\cdot)$.

List of Tables

4.1 ACD bounds for skew-symmetric dualities over $\mathbb{F}_{3^2}$ 50

4.2 Highest minimum distance for quaternary ACD codes with respect to non-symmetric dualities. 52

5.1 Highest minimum distance for quaternary one-rank hull codes with respect to non-symmetric dualities. 77