CONSTACYCLIC CODES

SAROJ RANI

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
DECEMBER 2016

CONSTACYCLIC CODES

by

SAROJ RANI

DEPARTMENT OF MATHEMATICS

Submitted

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

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI

DECEMBER 2016

Dedicated to

My Family and Supervisor

Certificate

This is to certify that the thesis entitled **"Constacyclic Codes"** submitted by **"Ms. Saroj Rani"** 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.

Dr. Anuradha Sharma
Assistant Professor
Department of Mathematics
Indian Institute of Technology Delhi

Acknowledgements

There are many ways of expressing one's gratitude towards someone. Language is one such way by means of which one can express one's gratefulness and indebtedness to one's guide and benefactors. Reaching foremost milestones in one's life does not occur without the assistance of many great people and for each one of them, I am truly blessed and obliged.

I would like to express my heartfelt gratitude to my supervisor, Dr. Anuradha Sharma, for her proficient supervision and research acumen. Above all and the most needed, she provided me unflinching encouragement and support in various ways. I am privileged to have the opportunity to work under her supervision. With her valuable suggestions, understanding, patience, enthusiasm, vivid discussions and above all with her friendly nature, she helped me in successfully completing my Ph.D. work. I am always being honored to have a teacher like her.

I am thankful to IIT Delhi authorities for providing me the necessary facilities and teaching assistantship for smooth completion of my research work. I express my regards to Prof. S. Dharmaraja, DRC Chairperson, for his love and support. Special thanks to my SRC (Student Research Committee) Members: Dr. Rupam Barman (Department of Mathematics), Dr. Ritumoni Sarma (Department of Mathematics) and Prof. S.D.Joshi (Department of Electrical Engineering) for generously sharing their time and knowledge. I'm also grateful to all faculty members of Department of Mathematics, IIT Delhi, for their cooperation and support.

Words cannot completely express my love and gratitude to my family who have supported and encouraged me during this journey. I would like to thank my parents for their life-long support and sacrifices, which sustained my interest in research and motivated me towards the successful completion of this study. My sincerest thanks to my brother Rajdeep and sister Santosh who have supported me through my difficult times with their inspiration and continous encouragement.

I will always remember the true friends who have walked with me on my path. There are too many to mention by name, yet too few to ever lose room for in my heart. Many thanks to my dear friends, especially of Neelam, Abhishek, Madhu, Shaily, Anju, Seema, Swati and Alka for times of laughter when I needed a reprieve from the intensity of research.

Finally, I thank the almighty God for the passion, strength, perseverance, and the resources to complete this study.

Saroj Rani

Abstract

Coding theory originated with the paper entitled 'A mathematical theory of communication' by Claude Shannon [66]. One of the objectives of coding theory is to design and study encoding and decoding schemes for reliable and faster transmission of messages across noisy communication channels. While passing through a noisy channel, some of the bits of the message may get distorted by noise and the receiver may receive a message different from the message that was sent. In order to detect or correct such errors, many families of error-correcting codes have been introduced and studied. The most-studied family of error-correcting codes is that of cyclic codes, which was first introduced and studied by Prange [63]. In a related direction, Berlekamp [15] introduced and studied negacyclic codes over the finite field $\mathbb{F}_p$, where $p \geq 5$ is a prime. In a subsequent work, Berlekamp [14] introduced and studied constacyclic codes over finite fields, which are generalizations of cyclic and negacyclic codes. These codes form an important family of error-correcting codes due to the following reasons: (i) many examples of good codes can be found within this family of codes, and (ii) these codes can be easily encoded and decoded (in principle) using shift registers due to their inherent algebraic structure. Recently, the problem of determination of (i) the algebraic structure of constacyclic codes over finite fields and their dual codes in terms of generator polynomials and (ii) all self-dual, self-orthogonal and complementary-dual constacyclic codes, has attracted a lot of attention. However, the algebraic structure of constacyclic codes over finite fields is known only in certain special cases.

In this thesis, we determine generator polynomials of all constacyclic codes of length $4\ell^m p^n$ over the finite field $\mathbb{F}_q$ with q elements, where p, ℓ are distinct odd primes, q is a power of the prime p and m, n are positive integers. We also determine their dual codes, and list all self-dual, self-orthogonal and complementary-dual constacyclic codes of length $4\ell^m p^n$ over $\mathbb{F}_q$. Besides this, we provide a method to list all constacyclic codes of length ℓp^w ($w \geq 0$ is an integer) over the finite field $\mathbb{F}_q$ with q elements, where q is a power of the prime p and ℓ is a positive integer coprime to q.

Recently, many important non-linear codes (e.g. Kerdock and Preparata codes) are related to linear codes over the ring of integers modulo 4 via the Gray map. This motivated many researchers to study constacyclic codes over finite rings. However, the algebraic structure of constacyclic codes is known only for some special lengths and over certain special classes of finite rings.

In this thesis, we determine all cyclic and negacyclic codes of length $4p^s$ over the finite commutative chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where p is an odd prime, $u^2 = 0$ and s, m are positive integers. We also determine their dual codes and list some self-dual cyclic and negacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Extending this work, we also determine all constacyclic codes of length $4p^s$ over the finite commutative chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where p is an odd prime, $u^2 = 0$ and s, m are positive integers. We also determine their dual codes and list some isodual constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$.

An important parameter of a constacyclic code is its (Hamming) weight distribution, which is a measure of its error performance relative to various communication channels. Therefore the problem of determination of weight distributions of constacyclic codes is of great interest. However, weight distributions of constacyclic codes are known only in a few cases. In this thesis, we explore this problem for an important class of constacyclic codes over fields, viz. irreducible constacyclic codes, which are building blocks of all the constacyclic codes over finite fields and have applications in deep space communications. More precisely, we provide a trace description for all the irreducible constacyclic codes of length n over the finite field $\mathbb{F}_q$, where n is a positive integer and q is a prime power coprime to n. As an application, we determine Hamming weight distributions of some irreducible constacyclic codes of length n over $\mathbb{F}_q$. We also derive a weight-divisibility theorem for irreducible constacyclic codes, and obtain both lower and upper bounds on the non-zero Hamming weights in irreducible constacyclic codes.

Contents

List of Tables

List of Symbols

Symbol	**Meaning**
$\lceil \cdot \rceil$	The *Ceiling* function
$\lfloor \cdot \rfloor$	The *Floor* function
$\cong$	is *isomorphic* to
$\equiv$	is *congruent* to
$< a >$	The *principal ideal* of a ring R generated by the element $a \in R$
$\gcd(a, b)$	The *greatest common divisor* of integers a and b
$\max\{a, b\}$	The *maximum* of real numbers a and b
$\min\{a, b\}$	The *minimum* of real numbers a and b
$\operatorname{lcm}[a, b]$	The *least common multiple* of integers a and b
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$\ell^r \mid\mid (q-1)$	r is the highest power of ℓ dividing $q-1$
$R[x]$	The ring of all polynomials in x over the ring R

$\deg f(x)$	The *degree* of the non-zero polynomial $f(x)$
w_H	The *Hamming* weight
$\mathbb{Z}_\ell$	The *residue class ring of integers modulo* ℓ
$\mathbb{F}_q$	The *finite field of order* q
$\mathbb{F}_q^*$	The *multiplicative group of* $\mathbb{F}_q$
ξ	A *primitive element* of $\mathbb{F}_q$
$\mathcal{C}^\perp$	The *dual code* of a linear code $\mathcal{C}$
$\mathrm{ann}(I)$	The *annihilator* of an ideal I
$\lvert A\rvert$	*Cardinality* of the set A
$O_n(q)$	The multiplicative order of q modulo n
ϕ	The Euler's phi function
$C_s^{(q,k)}$	The q-cyclotomic coset modulo k containing the integer s