# ADDITIVE CODES

TARANJOT KAUR


DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
AUGUST 2017

# ADDITIVE CODES

by


## TARANJOT KAUR

Department of Mathematics


*Submitted*

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

*to the*



Indian Institute of Technology Delhi

AUGUST 2017

*Dedicated to*

*my grandparents*

*my parents*

*and*

*my beloved sister Beeba*

# Certificate

This is to certify that the thesis entitled **"Additive codes"** submitted by **"Ms. Taranjot Kaur"** 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.

Date:

Place:

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

# Acknowledgements

*Knowledge and intellectual development are absolute necessity for one's sustainability and is a big challenge.*

*The enclosed thesis is a pursuit for knowledge and is made possible through the help, support and guidance of various people more specifically the dedicated educators from IIT Delhi. Achieving requisite milestone needs unceasing support from various people and my deepest gratitude to all.*

*I would like to express my overwhelming gratitude to my supervisor, Dr. Anuradha Sharma for her intellectual vigour and exemplary guidance throughout the duration of my research. My supervisor's valuable inputs, professional discussions and mentorship has really helped me in crossing this milestone of completing my thesis. I truly appreciate my supervisor Dr. Anuradha Sharma for giving me her time so generously. It has been a challenging experience and was indeed a privilege working with her.*

*I wish to acknowledge all the faculty members of Department of Mathematics, IIT Delhi for their support and co-operation. My special thanks are also extended to all the supporting staff who directly or indirectly have lent me their helping hand during my research period at IIT Delhi.*

*My sincere gratitude to SRC (Student Research Committee) members: Dr. Rupam Barman, Prof. S.D. Joshi and Dr. Ritumani Sarma for giving me their valuable time and suggestions.*

*I am grateful to National Board of Higher Mathematics (NBHM), Department of Atomic Energy, Mumbai for providing me with financial assistance.*

*I would also like to thank all my friends at IIT Delhi. My sincere thanks to my senior colleagues Amit Kumar Sharma, Dr. Swati Sidana, Anju, Seema and Swati Maheshwari for helping me as and*

*when required.*

*My deep sense of gratitude to the love, affection and support of both my grandmothers Mrs. Mohinder Kaur and Mrs. Tarlochan Kaur, and my late grandfathers who could not see me reach this stage. My warmest thanks to my dear parents Mr. Dalbir Singh and Mrs. Manna, my most beloved sister Beeba, my maternal uncle Rajan and my cousins Manmeet and Bisman for their unconditional and unceasing love and support which kept me going throughout my tough journey.*

*To you all, I dedicate this work. Thank you for being a part of my success story.*

*Above all I am grateful to almighty GOD for his kind eye and for always showering his uncountable blessings on me.*

*New Delhi* *Taranjot Kaur*

# Abstract

In 1948, Claude Shannon [43] published a classical paper entitled 'A mathematical theory of communication', which led to the birth of coding theory. Since then, many researchers have proposed various schemes for reliable transmission of data through noisy communication channels. Nowadays, error-correcting codes are widely used for transmission of images from deep space, storage of data, and designing registration numbers, etc. An algebraically-rich family of error-correcting codes is that of linear codes, which contains many well-known codes (e.g. Hadamard codes, Reed-Muller codes, etc.) and has elegant encoding and decoding procedures. The most studied class of linear codes is that of cyclic codes (e.g. Hamming codes, Reed-Solomon codes, BCH codes, etc.), which has a rich algebraic structure and can be effectively encoded and decoded using linear shift registers. Cyclic codes are further generalized to constacyclic codes by Berlekamp [2]. A natural generalization of linear codes is that of additive codes, which are first introduced and studied over the finite field $\mathbb{F}_4$ by Calderbank et al. [8]. They also provided several construction methods to construct quantum error-correcting codes from additive codes, due to which the study of additive codes have recently gained a great deal of attention. Analogous to the family of cyclic codes, many authors have introduced and studied cyclic additive codes over various finite commutative rings with unity. Towards this, Huffman [33] studied a class of cyclic additive codes, viz. cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes,

of length $n$, where $q$ is a power of the prime $p$, $n$ is a positive integer coprime to $q$ and $t \geq 2$ is an integer. In the same work, he studied their algebraic structure by writing a canonical form decomposition of these codes. Moreover, by placing ordinary and Hermitian trace bilinear forms on $\mathbb{F}_{q^t}^n$, he studied the algebraic structure of their dual codes, explicitly determined all self-dual and self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length $n$ when $t = 2$, and enumerated all self-dual and self-orthogonal cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length $n$ for any integer $t \geq 2$.

Let $q$ be a power of the prime $p$, $n$ be a positive integer coprime to $q$ and $t \geq 2$ be an integer. In this thesis, we introduce and study a new trace bilinear form, called the $*$ trace bilinear form, on $\mathbb{F}_{q^t}^n$, which is a generalization of the trace inner product considered by Calderbank et al. [8] and Hermitian trace inner product considered by Ezerman et al. [22]. We observe that $*$ trace bilinear form on $\mathbb{F}_{q^t}^n$ is non-degenerate for any integer $t \geq 2$ satisfying $t \not\equiv 1 \pmod{p}$. Furthermore, by placing $*$ trace bilinear form on $\mathbb{F}_{q^t}^n$, we

- study dual codes of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length $n$.
- explicitly determine basis sets of all self-orthogonal and self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length $n$ when $t = 2$.
- enumerate all self-orthogonal and self-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length $n$ for any integer $t \geq 2$.

Besides this, we introduce and study another important class of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes, viz. complementary-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length $n$. This class of cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes is analogous to the class of complementary-dual cyclic codes studied by Massey [39] and Yang and Massey [47]. By placing $*$, ordinary and Hermitian trace bilinear forms on $\mathbb{F}_{q^t}^n$, we

- explicitly determine basis sets of all complementary-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length $n$ when $t = 2$.

- enumerate all complementary-dual cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length $n$ for any integer $t \geq 2$.

In analogy with the family of constacyclic codes over finite fields, we also introduce and study the family of constacyclic additive codes, viz. constacyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length $n$, where $t \geq 2$ is an integer (not necessarily a prime number). This family of constacyclic additive codes contains cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes (cyclic additive codes) and negacyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes (negacyclic additive codes) as special cases. By placing $*$, ordinary and Hermitian trace bilinear form on $\mathbb{F}_{q^t}^n$, we

- study dual codes of constacyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length $n$.
- determine some isodual constacyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length $n$ when $t = 2$.
- explicitly determine basis sets of all self-orthogonal, self-dual and complementary-dual negacyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length $n$ when $t = 2$.
- enumerate self-dual, self-orthogonal and complementary-dual negacyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes of length $n$ for any integer $t \geq 2$.

# Contents

# List of Symbols

| **Symbol** | **Meaning** |
|---|---|
| $\|A\|$ | *Cardinality* of the set $A$ |
| $\max\{a, b\}$ | Maximum of real numbers $a$ and $b$ |
| $\mathbb{N}$ | The set of *Natural numbers* |
| $\gcd(a, b)$ | The *greatest common divisor* of integers $a$ and $b$ |
| $lcm(a, b)$ | The *least common multiple* of integers $a$ and $b$ |
| $a \equiv b \pmod{n}$ | The integers $a$ and $b$ are *congruent modulo a positive integer* $n$ |
| $\det A$ | The *determinant* of the matrix $A$ |
| $S_k$ | The *symmetric group* of $\{1, 2, \cdots, k\}$ |
| $D_k$ | The set of all *derangements* of $\{1, 2, \cdots, k\}$ |
| sgn | The *signum of a permutation* |
| $\mathbb{F}_Q$ | *The finite field* of order $Q$ |
| $\mathrm{Tr}_{Q,t}$ | The *trace map* from $\mathbb{F}_{Q^t}$ onto $\mathbb{F}_Q$ |
| $\begin{bmatrix} \cdot \\ \cdot \end{bmatrix}_Q$ | The *Q-binomial coefficient* or *Gaussian binomial coefficient* |

| | |
|---|---|
| $C_s^{(Q)}$ | The *Q-cyclotomic coset* containing the integer $s$ |
| $O_u(q)$ | The *multiplicative order* of integer $q$ modulo $u$ |
| $\langle u, v \rangle$ | The *subspace* of a vector space $V$ generated by vectors $u, v \in V$ |
| $\dim_F V$ | The *dimension* of a finite-dimensional vector space $V$ over the field $F$ |
| $\mathfrak{G}(\mathfrak{B})$ | The *Gram matrix* of a formed space $V$ with respect to the ordered basis $\mathfrak{B}$ of $V$ |
| $[\cdot, \cdot] \restriction_{U \times U}$ | The *restriction of the map* $[\cdot, \cdot]$ to $U \times U$ |