LINEAR COMPLEMENTARY DUAL CODES OVER FINITE COMMUTATIVE FROBENIUS RINGS

A Thesis Submitted
in
Partial Fulfillment of the Requirements
for the Degree of

Doctor of Philosophy

SANJIT BHOWMICK

(Roll no.: 17MA1108)

(Reg. no.: 19RMA045)

Under the Supervision

of

Dr SATYA BAGCHI, NIT DURGAPUR

Dr RAMAKRISHNA BANDI, IIIT NAYA RAIPUR



Department of Mathematics
National Institute of Technology Durgapur
West Bengal - 713209
India

September, 2022

Abstract

Error-correcting codes are often utilized in communication systems, data retrieval from deep space, data storage systems, etc. Coding theory is a branch of mathematics that deals with analyzing the algebraic structure of codes. The key factor in this area is to deploy sound principles which give reliable security in our daily communications. Mobiles and the internet have become an integral part of our daily life, and security and privacy are the most significant concerns in the digital era. So reliable and secure communication of information is a challenging problem for engineers and researchers. Let us consider a scenario where a country army has set up a camp to execute a remote machine in some rural area. When the officers at the headquarters receive some instructions, they must be careful about the following issues. Firstly, whether or not the instructions are received error-free. Secondly, whether or not the information sent from the headquarters is breached/altered during communication. Thirdly, protect the information from unauthorized persons during the communication. The first problem is about reliability, and the rest are about security and privacy. Coding theory addresses reliable communication, whereas cryptography deals with security. Coding theory and cryptography seem to achieve opposite goals initially, but sometimes they give the same. For instance, linear complementary dual (LCD) codes are secured from fault injection attacks and side-channel attacks. These applications of codes in cryptography have motivated the researchers to study and construct the codes which can be countermeasures to attacks. Although LCD codes over finite fields have been extensively studied so far, a little work has been done on LCD codes over finite rings. On the other hand, LCD codes over rings are an essential topic in coding theory because LCD codes over finite fields can be generalized as the equivalent to LCD codes over rings.

In this thesis, we study LCD codes over finite local rings. We also explicitly determine constacyclic LCD codes over finite chain rings. Our further discussion shows that non-free LCD codes don't exist over finite local rings. Using these results, we identify a necessary and sufficient condition for linear and cyclic LCD codes, respectively. We also study free cyclic LCD codes of any length over $\mathbb{Z}_4$ through group codes. Moreover, we explore the depth of the algebraic structure of LCD codes over finite commutative Frobenius rings. In addition, we explicitly determine non-free LCD codes over finite commutative Frobenius rings.

Apart from a theoretical illustration of LCD codes, we are focused on several applications of LCD codes. COVID-19 pandemic situation extends the necessity of Telecare Medicine Information Systems (TMIS) for patients and health workers to provide safe and effective healthcare services. Consequently, we propose a novel authentication

scheme based on LCD codes to ensure necessary security safeguards. Besides, the design of a multi-secret sharing scheme (MSSS) possesses security threats in cryptography. There are many MSSSs based on codes over finite fields in the literature. So, we provide MSSSs based on LCD codes over local rings. We also introduce a simple class of quantum codes called Entanglement Assisted Quantum Error-Correcting Codes (EAQECCs) from the LCD property of monomial-Cartesian codes.

Keywords: Linear codes, cyclic codes, constacyclic codes, linear complementary dual codes (LCD codes), matrix product codes (MP codes), finite chain rings, finite local rings, finite commutative Frobenius rings, projective modules, injective modules, TMIS and authentication schemes, EAQEC codes, multi-secret sharing scheme.