Abstract of Ph.D. Thesis

Name of the Scholar	**:**	**MAHESHANAND**
Name of Supervisor	**:**	**Prof. S. K. Wasan**
Department	**:**	**Mathematics**
Title of the Thesis	**:**	**A Study of Codes over Finite Rings**

ABSTRACT

Algebraic codes are of great interest to coding theorists, as they are easy to construct, encode and decode. Classically, algebraic codes have been mainly studied over finite fields. However, coding theorists for a long time had interest on codes over finite rings. Codes over finite rings got a serious attention in recent years after the breakthrough results by Hammons *et al.* (1994) that certain non-linear binary codes with good parameters are actually the binary images under the Gray map of some linear codes over $\mathbb{Z}_4$, the ring of integers modulo 4.

In this thesis, we have studied some families of algebraic codes over finite rings. These are cyclic codes, quasi-cyclic (QC) codes, constacyclic codes, quasi-twisted (QT) codes and Generalized Reed-Muller (GRM) codes. We have mainly focused to the study of QC codes, QT codes and GRM codes over $\mathbb{Z}_q$, $q = p^s$, p a prime number. Cyclic and constacyclic codes are studied briefly over Galois rings. We have established several structural properties of the aforementioned families of codes. The standard machinery of Galois rings is used to study these families of codes.

A necessary and sufficient condition for cyclic codes over Galois rings to be free is obtained, and a formula for their ranks is determined. A BCH bound for free cyclic codes over Galois rings defined by the roots of unity is also obtained.

QC codes of length lm and index l over $\mathbb{Z}_q$ are studied both in conventional row-circulant form and also as $\mathbb{Z}_q[x]/\langle x^m - 1\rangle$-submodules of $GR(q,l)[x]/\langle x^m - 1\rangle$, where $GR(q,l)$ is the Galois ring of of degree l over $\mathbb{Z}_q$ and $\langle x^m - 1\rangle$ denotes the ideal generated by $x^m - 1$. 1-generator QC codes over $\mathbb{Z}_q$ are discussed in detail. The form of the generator of a 1-generator QC code over $\mathbb{Z}_q$ is determined and a sufficient condition for such a code to be $\mathbb{Z}_q$-free is obtained. Some distance bounds for these codes are also discussed.

Constacyclic codes are an immediate generalization of cyclic codes. A factorization of $x^n - a$ over $\mathbb{Z}_q$, $a \in \mathbb{Z}_q^*$, is discussed, where $\mathbb{Z}_q^*$ is the set of invertible elements of $\mathbb{Z}_q$. It is shown that the residue class ring $GR(q,l)[x]/\langle x^n - a\rangle$, $a \in GR(q,l)^*$, is a principal ideal ring. Conditions for constacyclic codes over Galois rings to be free are discussed. A BCH bound for the free constacyclic codes over $GR(q,l)$, defined by the roots of $a \in GR(q,l)^*$, is obtained.

Quasi-twisted codes are a further generalization of QC codes. The structural properties of QT codes over $\mathbb{Z}_q$ are obtained. We have mainly focused to the 1-generator QT codes.

GRM codes are a generalization of binary Reed-Muller codes, in the sense that these codes are defined over arbitrary finite fields. These codes have rich algebraic and combinatorial structures. We have studied GRM codes over $\mathbb{Z}_q$ and established many of their structural properties. GRM codes defined here are a natural generalization of Quaternary Reed-Muller (QRM) codes defined in the literature. It has been shown that these codes are free codes over $\mathbb{Z}_q$, and formulas for their ranks are obtained. Kerdock and Preparata codes over $\mathbb{Z}_q$ are briefly discussed. A trace description of Kerdock codes over $\mathbb{Z}_q$ is given, and using it, we have obtained a trace description of GRM codes over $\mathbb{Z}_q$. For $0 \leq r < m(p-1)$, it is shown that the shortened GRM code $RM_{\mathbb{Z}_q}(r,m)^-$ is a free cyclic code over $\mathbb{Z}_q$, and the GRM code $RM_{\mathbb{Z}_q}(r,m)$ is the parity-check extension of $RM_{\mathbb{Z}_q}(r,m)^-$. A BCH bound for these codes, similar to the finite field case, is obtained. We have also given a multivariate description of these codes. Non-primitive GRM codes over $\mathbb{Z}_q$ are briefly discussed.

The entire thesis is divided into eight chapters.

Chapter 1 gives a brief introduction of the families of codes studied in the thesis and presents a literature survey on these codes. Chapter 2 is about basic concepts and covers most of the preliminary material. In Chapter 3 some properties of cyclic codes over Galois rings are studied. Chapter 4 is devoted to quasi-cyclic codes over $\mathbb{Z}_q$. We have mainly focused to 1-generator quasi-cyclic codes. Chapter 5 presents a study of constacyclic codes over Galois rings. In Chapter 6, quasi-twisted codes over $\mathbb{Z}_q$ are studied. It is shown that most properties of QT codes are analogous to that of QC codes. Chapter 7 presents a study of Generalized Reed-Muller codes over $\mathbb{Z}_q$. Chapter 8 is on conclusions and suggests some future research areas for the families of codes studied in the thesis. There are also two appendices in the thesis. Appendix A contains the tables of the Teichmüller sets of some Galois rings of small orders. Appendix B contains a brief discussion about the usual Hensel lifting method of the factorization of a polynomial over a commutative ring with identity.