

ABSTRACT

This study which examines BCH codes consist of six chapters.

Chapter 1 develops those concepts from Abstract Algebra that are necessary to an understanding of BCH codes. Finite fields and structure of finite fields are introduced in this chapter.

Chapter 2 is devoted to presentation of polynomials over finite fields. Construction of irreducible polynomials are also given.

Chapter 3 contains an introduction to coding theory. In this chapter linear codes, generator matrix of a code, dual code and parity-check matrix are considered.

Hamming codes are introduced in chapter 4.

The properties of cyclic codes, generator polynomial of cyclic codes are presented in chapter 5.

Chapter 6 covers in detail BCH codes. Primitive element, primitive polynomial and minimal polynomials are examined. A class of BCH codes for t -error correction is presented. Further, in this chapter the new developments of BCH codes and Goppa codes are presented.

Key Words: Finite fields, roots of unity and cyclotomic polynomials, order of polynomials, irreducible polynomials, linear codes, Hamming codes, cyclic codes, generator polynomial, primitive element, primitive polynomial, minimal polynomials, designed distance, BCH codes, Reed-Solomon codes, Goppa codes.

ÖZET

BCH kodlarının ele alındığı bu çalışma, altı bölümden oluşmaktadır.

Bölüm 1’de BCH kodları için gerekli cebirsel bilgiler verilmiştir. Sonlu cisimler ve sonlu cisimlerin yapısı incelenmiştir.

Bölüm 2’de sonlu cisimler üzerinde polinomlardan söz edilmiş, indirgenemez polinomların kuruluşu ele alınmıştır.

Bölüm 3’te kodlar teorisine bir giriş yapılmıştır. Bu bölümde lineer kodlar, bir kodun üreteç matrisi, dual kod ve eşlik-denetim (parity-check) matrisi incelenmiştir.

Bölüm 4’te Hamming kodlarından söz edilmiştir.

Bölüm 5’te devresel kodların özellikleri, devresel kodların üreteç polinomu gösterilmiştir.

Bölüm 6’da BCH kodları detaylı bir şekilde incelenmiştir. Primitif eleman, primitif polinom ve minimal polinomlar anlatılmıştır. t – hata düzelten BCH kodlarının bir sınıfı ele alınmıştır. Ayrıca bu bölümde, BCH kodları hakkındaki son gelişmeler ve Goppa kodları anlatılmıştır.

Anahtar kelimeler: Sonlu cisimler, birimin kökleri ve cyclotomic polinomlar, polinomların mertebesi, indirgenemez polinomlar, lineer kodlar, Hamming kodları, devresel kodlar, üreteç polinomu, primitif eleman, primitif polinom, minimal polinomlar, tasarlanmış mesafe, BCH kodları, Reed-Solomon kodu, Goppa kodları.