OLIVER PRETZEL
Imperial College, London

Error-Correcting Codes and Finite Fields

Student edition

CLARENDON PRESS · OXFORD

Contents

PART 1 BASIC CODING THEORY

1 Introduction 3

Errors of transmission. Examples from natural language. Channel models. The binary symmetric channel. Three simple codes (a parity check code, a triple repetition code, and a triple parity check code).

2 Block codes, weight, and distance 13

Block codes. Block length, message block length, and rate. Definition of Hamming weight and distance. Minimum distance, error detection, and error correction. Block and message success probabilities. Calculation of error detection/correction probabilities for the examples of Chapter 1. Discussion of Shannon's theorem (without proof).

3 Linear codes 27

Definition of linear codes and fields. Dimension and rate. The generator matrix. Standard form generator matrices and systematic encoding. Message and check bits. The check matrix. Uniqueness of standard form generator and check matrices.

4 Error processing for linear codes 47

Decoding by cosets (standard array). Coset leaders and syndromes. Code can correct single errors if and only if check matrix has distinct non-zero columns. Conditions for multiple error correction.

5 Hamming codes and the binary Golay codes 63

Definition of the sequence of binary Hamming codes Ham(k) by their check matrices. Success probabilities for Hamming codes. Long Hamming codes are very efficient, but poor at correcting errors. Perfect codes. Construction of the binary Golay codes by Turyn's method.

Appendix LA Linear algebra 79

The laws of arithmetic: rings, domains, and fields. Elementary vector space theory. Bases and dimension. Elementary matrix theory. Row operations, rank, and nullity. Vandermonde matrices.

PART 2 FINITE FIELDS

6 Introduction and an example **95**

The need for fields other than $\mathbf{Z}/2$. An attempt to construct a field of order 16. $\mathbf{Z}/16$ will not do. Polynomial arithmetic. Table of $GF(16)$.

7 Euclid's algorithm **106**

Division with remainder. Euclidean domains with $F[x]$ and $\mathbf{Z}$ as examples. Euclid's algorithm in tabular form for a Euclidean domain. Finding the highest common factor in the form $(a, b) = ua + vb$.
Extras. Relations between entries in the table for Euclid's algorithm. Continued fractions. Convergents, the entries in the tabular form of Euclid's algorithm and convergents to continued fractions.

8 Invertible and irreducible elements **122**

Definition of invertible elements in a Euclidean domain. Definition of irreducible elements in a Euclidean domain. The 1-trick and the key property of irreducible elements. Discussion of unique factorization.
Extras. Proof of unique factorization.

9 The construction of fields **136**

Construction of the factor ring (residue class ring) D/a. D/a is a field if and only if a is irreducible. Using Euclid's algorithm to perform field arithmetic in $F[x]/f(x)$. Examples: $GF(16)$ as $GF(2)[x]/(x^4 + x^3 + 1)$, $\mathbf{Z}/787$.

10 The structure of finite fields **151**

The prime field and the characteristic. The order of a finite field. The Frobenius automorphism $x \to x^p$. Fermat's little theorem: if F has order q then all its elements are roots of $x^q - x$. Example: $GF(16)$.

11 Roots of polynomials **166**

The evaluation map. Its basic properties (i.e. it is a homomorphism). The formal derivative. Horner's scheme for evaluating a polynomial. Extension of Horner's scheme to evaluate the derivative. Multiple roots. The minimal polynomial of α. Characterization of the minimal polynomial and the set (ideal) of polynomials with α as a root. List of minimal polynomials of elements of $GF(16)$. Isomorphism $F[\alpha] \cong F[x]/mp_\alpha(x)$. Construction of a field containing a root of a given polynomial. Existence of finite fields of all legal orders.
Extras. Calculation of the minimum polynomial of β using the Frobenius automorphism.

12 Primitive elements 179

Definition of primitive elements. Primitive elements of $GF(16)$. Logarithms for calculating products and quotients in finite fields. Zech logarithms for calculating sums. Primitive polynomials. Existence of primitive elements. Existence of subfields of all legal orders. Isomorphism of fields of the same order. The polynomial $x^q - x$ is the product of all irreducible polynomials of degree dividing q.
Extras. The number of irreducible polynomials of a given degree.

Appendix PF Polynomials over a field 191

Recapitulation of the basic theory of polynomials over a field. Definition, addition, multiplication, degree. $F[x]$ is an integral domain. Division with remainder. Polynomials in two indeterminates.

PART 3 BCH CODES AND OTHER POLYNOMIAL CODES

13 BCH codes as subcodes of Hamming codes 201

Example: BCH(4, 2) constructed from Ham(4) by extending the check matrix H_4. Extensions must not be linear (or quadratic). View H_k as having entries in $GF(2^k)$. Criterion for multiple error correction. Vandermonde matrices. The full check matrix $V_{4,3}$ and the reduced check matrix $H_{4,3}$ ($V_{k,t}$ and $H_{k,t}$ in general). Example BCH(4, 3). BCH(k, t) can correct t errors per block. It has block length $2^k - 1$ and dimension $\geqslant 2^k - 1 - kt$.

14 BCH codes as polynomial codes 216

Example: BCH(4, 3) used throughout to illustrate the theory. Code words as polynomials. Redefine BCH(k, t) in terms of polynomials. The generator polynomial of BCH(k, t). Dimension of BCH(k, t). Encoding by multiplication. The check polynomial of BCH(k, t). Use of the check polynomial, to verify and decode a code word. Systematic encoding by division with remainder.
Extras. Polynomial codes in general. Cyclic codes in general. Recognition of polynomial and cyclic codes.

15 BCH error correction: (1) the fundamental equation 233

Example BCH(4, 3) continued. The error polynomial and error locations. Syndromes: calculation via Horner's scheme. Direct solution of case of two errors. The syndrome polynomial. Derivation of the fundamental equation. The error locator, error evaluator and error co-evaluator polynomials. Uniqueness of these as solutions of the fundamental equation.

16 BCH error correction: (2) an algorithm **249**

Example BCH(4, 3) continued. The Sugiyama–Kasahara–Hirasawa–Namekawa error processor using Euclid's algorithm. Failure modes of the algorithm.

17 Reed–Solomon codes and burst error correction **267**

Example RS(4, 3) used throughout. The Reed–Solomon code RS(k, t) corresponding to BCH(k, t). Adaptation of the decoding algorithm to RS(k, t). Failure modes. RS(k, t) as a cyclic code over $GF(2^k)$. Parameters of RS(k, t) over $GF(2^k)$ and $GF(2)$. RS(k, t) as a burst error-correcting code. Comparison with interleaved BCH(k, t).
Extras. Detailed proofs of the statements concerning error modes.

18 Bounds on codes **287**

Extending, shortening and puncturing a code. The Singleton bound. MDS codes. Reed–Solomon codes are MDS. Coding bounds based on sphere packing: the Hamming bound, the Gilbert–Varshamov bound. The asymptotic Gilbert–Varshamov bound.

Good and bad families of codes. BCH codes are bad in relation to their designed distance, although their parameters for moderate block lengths are good. Estimates for the true minimum distance. Discussion of the fact that BCH codes are still bad for their true minimum distance.
Extras. Proof of the estimates used in establishing the asymptotic Gilbert–Varshamov bound.

PART 4 CLASSICAL GOPPA CODES

19 Classical Goppa codes **303**

Definition of the Goppa Code $GC(P, g)$ with Goppa polynomial $g(x)$. Rational functions over $GF(q)$. Dimension of $GC(P, g)$, special case of binary Goppa codes. Minimum distance of the $GC(P, g)$. Goppa codes and codes of BCH-type.

20 Classical Goppa codes: error processing **320**

The error locator and error evaluator polynomials, the fundamental equation. Euclid's algorithm decoding for $GC(P, g)$.
Extras. Classical Goppa codes are bad for their designed distance, but there exists a sequence of classical Goppa codes that is good for the true minimum distance.

Bibliography **333**

Index **337**