

1. Record Nr.	UNINA9910139339603321
Autore	Adamek Jiri <1947->
Titolo	Foundations of coding : theory and applications of error-correcting codes, with an introduction to cryptography and information theory // Jiri Adamek
Pubbl/distr/stampa	Chichester ; ; New York, : Wiley, c1991
ISBN	9786613813954 9781282253308 1282253301 9781118033265 1118033264 9781118031513 1118031512
Descrizione fisica	1 online resource (356 p.)
Disciplina	003/.54
Soggetti	Coding theory Algebra
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Foundations of Coding: Theory and Applications of Error-Correcting Codes with an Introduction to Cryptography and Information Theory; Contents; CONTENTS; Introduction; Part I Coding and Information Theory; 1 Coding and Decoding; 1.1 Coding; 1.2 Unique Decoding; 1.3 Block Codes and Instantaneous Codes; 1.4 Some Important Block Codes; 1.5 Construction of Instantaneous Codes; 1.6 Kraft's Inequality; 1.7 McMillan's Theorem; Exercises; Notes; 2 Huffman Codes; 2.1 Information Source; 2.2 Huffman Codes; 2.3 Construction of Binary Huffman Codes; 2.4 Example; 2.5 Construction of General Huffman Codes ExercisesNotes; 3 Data Compression and Entropy; 3.1 An Example of Data Compression; 3.2 The Idea of Entropy; 3.3 The Definition of Entropy; 3.4 An Example; 3.5 Maximum and Minimum Entropy; 3.6 Extensions of a Source; 3.7 Entropy and Average Length; 3.8 Shannon's Noiseless Coding Theorem; 3.9 Concluding Remarks; Exercises; Notes;

4 Reliable Communication Through Unreliable Channels; 4.1 Binary Symmetric Channels; 4.2 Information Rate; 4.3 An Example of Increased Reliability; 4.4 Hamming Distance; 4.5 Detection of Errors; 4.6 Correction of Errors; 4.7 Channel Capacity
4.8 Shannon's Fundamental Theorem Exercises; Notes; Part II Error-Correcting Codes; 5 Binary Linear Codes; 5.1 Binary Addition and Multiplication; 5.2 Codes Described by Equations; 5.3 Binary Linear Codes; 5.4 Parity Check Matrix; 5.5 Hamming Codes-Perfect Codes for Single Errors; 5.6 The Probability of Undetected Errors; Exercises; Notes; Notes; 6 Groups and Standard Arrays; 6.1 Commutative Groups; 6.2 Subgroups and Cosets; 6.3 Decoding by Standard Arrays; Exercises; 7 Linear Algebra; 7.1 Fields and Rings; 7.2 The Fields \mathbb{Z}_p ; 7.3 Linear Spaces; 7.4 Finite-Dimensional Spaces; 7.5 Matrices
7.6 Operations on Matrices 7.7 Orthogonal Complement; Exercises; Notes; 8 Linear Codes; 8.1 Generator Matrix; 8.2 Parity Check Matrix; 8.3 Syndrome; 8.4 Detection and Correction of Errors; 8.5 Extended Codes and Other Modifications; 8.6 Simultaneous Correction and Detection of Errors; 8.7 MacWilliams Identity; Exercises; Notes; 9 Reed-Muller Codes: Weak Codes with Easy Decoding; 9.1 Boolean Functions; 9.2 Boolean Polynomials; 9.3 Reed-Muller Codes; 9.4 Geometric Interpretation: Three-Dimensional Case; 9.5 Geometric Interpretation: General Case; 9.6 Decoding Reed-Muller Codes; Exercises; Notes
10 Cyclic Codes 10.1 Generator Polynomial; 10.2 Encoding Cyclic Codes; 10.3 Parity Check Polynomial; 10.4 Decoding Cyclic Codes; 10.5 Error-Trapping Decoding; 10.6 Golay Code: A Perfect Code for Triple Errors; 10.7 Burst Errors; 10.8 Fire Codes: High-Rate Codes for Burst Errors; Exercises; Notes; 11 Polynomials and Finite Fields; 11.1 Zeros of Polynomials; 11.2 Algebraic Extensions of a Field; 11.3 Galois Fields; 11.4 Primitive Elements; 11.5 The Characteristic of a Field; 11.6 Minimal Polynomial; 11.7 Order; 11.8 The Structure of Finite Fields; 11.9 Existence of Galois Fields; Exercises
Notes

Sommario/riassunto

Although devoted to constructions of good codes for error control, secrecy or data compression, the emphasis is on the first direction. Introduces a number of important classes of error-detecting and error-correcting codes as well as their decoding methods. Background material on modern algebra is presented where required. The role of error-correcting codes in modern cryptography is treated as are data compression and other topics related to information theory. The definition-theorem proof style used in mathematics texts is employed through the book but formalism is avoided wherever possible.
