

<<信息论、编码与密码学>>

图书基本信息

书名：<<信息论、编码与密码学>>

13位ISBN编号：9787111127703

10位ISBN编号：7111127706

出版时间：2003-9

出版时间：机械工业出版社

作者：Ranjan Bose

页数：277

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<信息论、编码与密码学>>

### 内容概要

大多数介绍信息论和编码学的书，不是太过学术化，就是太过简单。

本书避免了上述缺点，既考虑到了数学的严谨性，又充分考虑了易读性。

本书的主要特点 详细介绍了网格编码调制(TCM) . 并重点介绍了加性高斯白噪声(AWGN)和衰退倍道。

以大量示例仔细描述了信源编码。

深入讨论了TurboCode。

简要介绍了线性代数。

通过精心挑选的115道例题及115道练习题，清晰透彻地讲解了深奥的理论和定义。

通过大量篇幅论述了密码学，包括基本原理。

私钥和公钥密码，当今通用的加密标准及最新发展趋势。

“叙述流畅，通过大量示例及精确的解说透彻地论述了各个主题。

”——审稿人 作者简介 Ranjan Bose 宾夕法尼亚大学获得博士学位，现在是德里印度理工大学的副教授，他曾任加州 圣何塞的联合半导体公司的高级设计工程师。

## 书籍目录

Preface Acknowledgements Part I Information Theory and Source Coding 1. Source Coding 31.1 Introduction to Information Theory 31.2 Uncertainty And Information 41.3 Average Mutual Information And Entropy 111.4 Information Measures For Continuous Random Variables 141.5 Source Coding Theorem 151.6 Huffman Coding 211.7 The Lempel-Ziv Algorithm 281.8 Run Length Encoding and the PCX Format 301.9 Rate Distortion Function 331.10 Optimum Quantizer Design 361.11 Introduction to Image Compression 371.19 TheJpeg Standard for Lossless Compression 381.13 TheJpeg Standard for Lossy Compression 391.14 Concluding Remarks 41Summary 42Problems 44Computer Problems 462. Channel Capacity and Coding 472.1 Introduction 472.2 Channel Models 482.3 Channel Capacity 502.4 Channel Coding 522.5 Information Capacity Theorem 562.6 The Shannon Limit 592.7 Random Selection of Codes 612.8 Concluding Remarks 67Summary 68Problems 69Computer Problems 71Part II Error Control Coding(Channel Coding)3. Linear Block Codes for Error Correction 753.1 Introduction to Error Correcting Codes 753.2 Basic Definitions 773.3 Matrix Description of Linear Block Codes 813.4 Equivalent Codes 823.5 Parity Check Matrix 853.6 Decoding of a Linear Block Code 873.7 Syndrome Decoding 943.8 Error Probability after Coding (Probability of Error Correction) 953.9 Perfect Codes 973.10 Hamming Codes 1003.11 Optimal Linear Codes 1023.12 Maximum Distance Separable (MDS) Codes 1023.13 Concluding Remarks 102Summary 103Problems 105Computer Problems 1064. Cyclic Codes 1084.1 Introduction to Cyclic Codes 1084.2 Polynomials 1094.3 The Division Algorithm for Polynomials 1104.4 A Method for Generating Cyclic Codes 1154.5 Matrix Description of Cyclic Codes 1194.6 Burst Error Correction 1214.7 Fire Codes 1234.8 Golay Codes 1244.9 Cyclic Redundancy Check (CRC) Codes 1254.10 Circuit Implementation of Cyclic Codes 1284.11 Concluding Remarks 132Summary 132Problems 134Computer Problems 1355. Bose-Chaudhuri Hocquenghem (BCH) Codes5.1 Introduction to BCH Codes 1365.2 Primitive Elements 1375.3 Minimal Polynomials 1335.4 Generator Polynomials in Terms of Minimal Polynomials 1415.5 Some Examples of BCH Codes 1435.6 Decoding of BCH Codes 1475.7 Reed-Solomon Codes 1505.8 Implementation of Reed-Solomon Encoders and Decoders 1535.9 Nested Codes 1535.10 Concluding Remarks 155Summary 156Problems 157Computer Problems 1586. Convolutional Codes6.1 Introduction to Convolutional Codes 1596.2 Tree Codes and Trellis Codes 1606.3 Polynomial Description of Convolutional Codes(Analytical Representation) 1656.4 Distance Notions for Convolutional Codes 1706.5 The Generating Function 1736.6 Matrix Description of Convolutional Codes 7766.7 Viterbi Decoding of Convolutional Codes 1786.8 Distance Bounds for Convolutional Codes 1856.9 Performance Bounds 1876.10 Known Good Convolutional Codes 1886.11 Turbo Codes 1906.12 Turbo Decoding 1926.13 Concluding Remarks 198Summary 199Problems 201Computer Problems 2037. Trellis Coded Modulation 2067.1 Introduction to TCM 2067.2 The Concept of Coded Modulation 2077.3 Mapping by Set Partitioning 2127.4 Ungerboeck's TCM Design Rules 2167.5 Tcm Decoder 2207.6 Performance Evaluation for Awgn Channel 2217.7 Computation of dfree 2277.8 Tcm for Fading Channels 2287.9 Concluding Remarks 232Summary 233Problems 234Computer Problems 238Part IIICoding for Secure Communications8. Cryptography 2418.1 Introduction to Cryptography 2418.2 An Overview of Encryption Techniques 2428.3 Operations Used By Encryption Algorithms 2458.4 Symmetric (Secret Key) Cryptography 2468.5 Data Encryption Standard (DES) 2488.6 International Data Encryption Algorithm (IDEA) 2528.7 RC Ciphers 2538.8 Asymmetric (Public-Key) Algorithms 2548.9 The RSA Algorithm 2548.10 Pretty Good Privacy (PGP) 2568.11 One-Way Hashing 2538.12 Other Techniques 2608.13 Secure Communication Using Chaos Functions 2618.14 Cryptanalysis 2628.15 Politics of Cryptography 2648.16 Concluding Remarks 265Summary 268Problems 269Computer Problems 271Index 273

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>