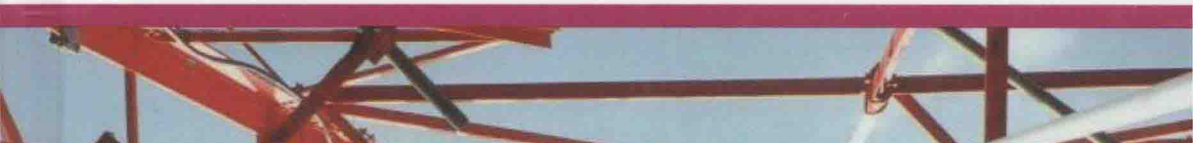
FOUNDATIONS OF CODING

Compression, Encryption, Error Correction



Jean-Guillaume Dumas • Jean-Louis Roch
Éric Tannier • Sébastien Varrette

WILEY

FOUNDATIONS OF CODING

Compression, Encryption, Error Correction

JEAN-GUILLAUME DUMAS
Université de Grenoble

JEAN-LOUIS ROCH
Université de Grenoble

ÉRIC TANNIER
Inria, Université de Lyon

SÉBASTIEN VARRETTE
Université du Luxembourg

常州大学图书馆
藏书章

WILEY

Copyright © 2015 by John Wiley & Sons, Inc. All rights reserved

Published by John Wiley & Sons, Inc., Hoboken, New Jersey
Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Dumas, Jean-Guillaume.
Foundations of coding : compression, encryption, errorcorrection / Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier, Sebastien Varrette.
pages cm
Includes bibliographical references and index.
ISBN 978-1-118-88144-6 (cloth)
1. Coding theory. I. Roch, Jean-Louis (Mathematician) II. Tannier, Eric. III. Varrette, Sebastien. IV. Title.
TK5102.92.D86 2015
003′.54–dc23

2014039504

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

FOUNDATIONS OF CODING

此为试读,需要完整PDF请访问: www.ertongbook.com

FOREWORD

This work has been initiated in spring 2000 with the creation of the joint ENSIMAG-ENSERG Telecommunication department at the National Polytechnic Institute of Grenoble (INPG – France) and the setting up of a general course (last year French Licence level in the Licence-Master-Doctorate scheme) providing an introduction to codes and their applications.

Although it was initially published as a handout, it evolved and became reference material for several courses in Grenoble universities – both in the INPG and in the Joseph Fourier University (UJF) at the master level.

We take this occasion to thank our colleagues who participated in these courses and helped us improve our material with their remarks: Gilles Debunne, Yves Denneulin, Dominique Duval, Grégory Mounié and Karim Samaké.

In 2007, a book was published in French by Dunod editions in their mathematics and computer science collection. It was then reprinted, with a few amendments, in the beginning of 2009, and edited in an augmented version in 2013.

Éric Bourre, Cécile Canovas-Dumas, Mélanie Favre, Françoise Jung, Madeline Lambert, Benjamin Mathon, Marie-Aude Steineur, and Antoine Taveneaux participated to these first two editions by reading the drafts and spotting some mistakes.

This English edition was started in 2009, when our colleagues Rodney Coleman and Romain Xu undertook the task of translating the 352 pages of the French edition in English. Let them be gratefully thanked here.

Compared to this translation, this book has been revised and significantly augmented (20% additional pages and 27 new exercises). We now cover modern and frequently used techniques, as elliptic curves, low density codes, or matrix bar-codes as well as new standards like the eSTREAM portfolio, Galois hashing and counter mode, and the new standard hashing algorithm 3, Keccak. In addition, we have updated several parts, including steganography and watermarking, maximum likelihood decoding, saturation attacks (on AES), and postquantum cryptography.

"Foundations of Coding: Compression, Encryption, Error Correction" comes now with a companion website http://foundationsofcoding.imag.fr. This web site provides access to tools, resources, and news about the book, and, more generally, about security. In particular, we propose interactive solutions to several exercises via worksheets, using the free mathematical software Sage.

GRENOBLE, LYON, LUXEMBOURG
JEAN-GUILLAUME DUMAS, JEAN-LOUIS ROCH,
ÉRIC TANNIER, SÉBASTIEN VARRETTE.

CONTENTS

List of Figures, Tables, Algorithms and Acronyms ix

Foreword xvii

Introduction 1

1 Foundations of Coding 5

1.1 From Julius Caesar to Telecopy, 6
1.1.1 The Source: from an Image to a Sequence of Pixels, 6
1.1.2 Message Compression, 7
1.1.3 Error Detection, 8
1.1.4 Encryption, 9
1.1.5 Decryption, 9
1.1.6 Drawbacks of the Fax Code, 11
1.1.7 Orders of Magnitude and Complexity Bounds for Algorithms, 12
1.2 Stream Ciphers and Probabilities, 15
1.2.1 The Vernam Cipher and the One-Time-Pad Cryptosystem, 15
1.2.2 Some Probability, 16
1.2.3 Entropy, 18
1.2.4 Steganography and Watermarking, 23
1.2.5 Perfect Secrecy, 24
1.2.6 Perfect Secrecy in Practice and Kerckhoffs' Principles, 24
1.3 Block Ciphers, Algebra, and Arithmetic, 26
1.3.1 Blocks and Chaining Modes from CBC to CTR, 27
1.3.2 Algebraic Structure of Codewords, 30

1.3.3 Bijective Encoding of a Block, 35
1.3.4 Construction of Prime Fields and Finite Fields, 43
1.3.5 Implementation of Finite Fields, 52
1.3.6 Curves Over Finite Fields, 57
1.3.7 Pseudo-Random Number Generators (PRNG), 62
1.4 Decoding, Decryption, Attacks, 68
1.4.1 Decoding without Ambiguity, 68
1.4.2 Noninjective Codes, 73
1.4.3 Cryptanalysis, 84

2 Information Theory and Compression 99

2.1 Information Theory, 100
2.1.1 Average Length of a Code, 100
2.1.2 Entropy as a Measure of the Amount of Information, 101
2.1.3 Shannon's Theorem, 102
2.2 Statistical Encoding, 104
2.2.1 Huffman's Algorithm, 104
2.2.2 Arithmetic Encoding, 109
2.2.3 Adaptive Codes, 114
2.3 Heuristics of Entropy Reduction, 117
2.3.1 Run-Length Encoding (RLE), 117
2.3.2 Move-to-Front, 119
2.3.3 Burrows–Wheeler Transform (BWT), 120
2.4 Common Compression Codes, 122
2.4.1 Lempel–Ziv's Algorithm and `gzip` Variants, 123
2.4.2 Comparisons of Compression Algorithms, 126
2.4.3 GIF and PNG Formats for Image Compression, 127
2.5 Lossy Compression, 128
2.5.1 Deterioration of Information, 128
2.5.2 Transformation of Audiovisual Information, 128
2.5.3 JPEG Format, 129
2.5.4 Motion Picture Experts Group (MPEG) Format, 133

3 Cryptology 136

3.1 General Principles, 137
3.1.1 Terminology, 137
3.1.2 What is the Use of Cryptography? 138
3.1.3 Main Types of Threats, 139
3.2 Secret Key Cryptography, 141
3.2.1 Principle of Symmetric Cryptography, 141
3.2.2 Classes of Symmetric Encryption Schemes, 143
3.2.3 Data Encryption Standard (DES) System, 145
3.2.4 Rijndael: Advanced Encryption Standard (AES), 151

3.3 Key Exchange, 161
3.3.1 Diffie–Hellman Protocol and Man-in-the-Middle Attacks, 161
3.3.2 Kerberos: a Secret Key Provider, 163
3.4 Public Key Cryptography, 167
3.4.1 Motivations and Main Principles, 167
3.4.2 Rivest–Shamir–Adleman (RSA) Encryption, 169
3.4.3 El Gamal Encryption, 174
3.5 Authentication, Integrity, Nonrepudiation, Signatures, 175
3.5.1 Cryptographic Hash Functions, 176
3.5.2 Public Key Authentication, 186
3.5.3 Electronic Signatures, 187
3.6 Key Management, 192
3.6.1 Generation of Cryptographically Secure Bits, 192
3.6.2 Public Key Infrastructure (PKI), 192
3.6.3 Securing Channels with the SSH Tool, 203

4 Error Detection and Correction 209

4.1 Principle of Error Detection and Error Correction, 211
4.1.1 Block Coding, 211
4.1.2 A Simple Example of Parity Detection, 211
4.1.3 Correction Using Longitudinal and Transverse Parity, 212
4.1.4 Encoding, Decoding, and Probability of Error, 213
4.1.5 Shannon's Second Theorem, 214
4.2 Error Detection by Parity – CRC Codes, 218
4.2.1 Parity Check on Integers: ISBN, EAN, LUHN, 218
4.2.2 Cyclic Redundancy Checks (CRC), 221
4.3 Distance of a Code, 222
4.3.1 Error Correction Code and Hamming Distance, 222
4.3.2 Equivalent Codes, Extended Codes, and Shortened Codes, 227
4.3.3 Perfect Codes, 229
4.3.4 Binary Hamming Codes, 230
4.4 Linear Codes and Cyclic Codes, 232
4.4.1 Linear Codes and Minimum Redundancy, 232
4.4.2 Encoding and Decoding of Linear Codes, 234
4.4.3 Low Density Parity Check (LDPC) Codes, 238
4.4.4 Cyclic Codes, 250
4.4.5 Bose–Chaudhuri–Hocquenghem (BCH) Codes, 254
4.4.6 Optimal BCH Codes: Reed–Solomon Codes, 256
4.5 Bursts of Errors and Interleaving, 262
4.5.1 Packets of Errors, 262
4.5.2 Interleaving, 263
4.5.3 Interleaving with Delay and Interleaving Table, 264
4.5.4 Cross-Interleaved codes, 265

此为试读,需要完整PDF请访问: www.ertongbook.com

4.6 Convolutional Codes and Turbo Codes, 268
4.6.1 Encoding by Convolution, 268
4.6.2 Shortest Path Decoding, 269
4.6.3 Turbo Codes, 273

Compression, Encryption, Correction: As a Conclusion **277**

Problem Solutions **281**

Bibliography **343**

Index **345**

LIST OF FIGURES, TABLES, ALGORITHMS AND ACRONYMS

List of Figures

I.1 Fundamental coding scheme 2
I.2 Notions introduced in Chapter 1 4

1.1 Spartan Scytale principle to transmit the text "HELLOWORLD" 10
1.2 Bitwise encryption (Stream cipher) 25
1.3 Block ciphers: ECB mode 28
1.4 Block ciphers: CBC mode 28
1.5 Block ciphers: CFB mode 28
1.6 Block ciphers: OFB mode 29
1.7 Block ciphers: CTR mode 29
1.8 Principle of a one-way function 43
1.9 (a) Elliptic curve addition and (b) doubling on $y^2 = x^3 - x\sqrt[3]{2}$ 60
1.10 Functional diagram of an LFSR 64
1.11 *Bluetooth* encryption 65
1.12 Example of a Huffman tree 72
1.13 Principle of a hash function 75
1.14 Compression function of a hash function 76
1.15 Merkle–Damgård construction 76
1.16 Davies–Meyer construction 77
1.17 Miyaguchi–Preneel construction 78
1.18 Fourier transform 79
1.19 Discrete Fourier Transform (DFT) 80

1.20 Discrete Cosine Transform (DCT) 80
1.21 Floyd's cycle detection, in the form of a rho 91

2.1 Huffman encoding: beginning of the algorithm 104
2.2 Huffman's encoding: first step ($q = 2$) 104
2.3 Example of a construction of the Huffman code 106
2.4 Fax code 119
2.5 BWT on COMPRESSED 121
2.6 bzip2 122
2.7 The 8 × 8 RGB image with white background (here in gray-levels) 130
2.8 Joint Photographic Experts Group (JPEG) zigzag scan 131
2.9 JPEG compression 131
2.10 MPEG-1 compression 134
2.11 MP3 sound compression 135

3.1 Fundamental relation of cryptography 137
3.2 Principle of an integrity checking algorithm 138
3.3 Principle of symmetric cryptography 141
3.4 Stream cipher 143
3.5 Block cipher 145
3.6 One round of DES 146
3.7 DES: Function f 147
3.8 DES key derivation 148
3.9 Matricial representation of a 16-byte block 153
3.10 `SubBytes` operation in AES 155
3.11 `ShiftRows` stage in AES 156
3.12 `MixColumns` operation in AES 157
3.13 `KeySchedule` operation in AES 158
3.14 Representation of the expanded key `W` as a sequence of columns 158
3.15 Kerberos authentication steps 164
3.16 Principle of public key encryption 168
3.17 History of the main hash functions 176
3.18 Rounds 1, 2, 3, and 4 in MD5 ($0 \leq i \leq 63$) 178
3.19 Round i in SHA-1 ($0 \leq i \leq 79$) 179
3.20 Keccak's sponge construct (SHA-3) 181
3.21 Integrity check with hash functions using a secure channel 182
3.22 Integrity check with hash functions using an encryption function 183
3.23 Optimal Asymmetric Encryption Padding (OAEP) 184
3.24 Principle of the use of an MAC 185
3.25 Message Authentication Code (MAC) using symmetric encryption 185
3.26 Principle of public key signatures and verification 188
3.27 Principle of the creation of certificates 193
3.28 Issuing a certificate 194
3.29 Generation and content of an X.509 certificate 196
3.30 Verification of certificate and public key extraction 197

3.31 PKI model for X-509 certificates 198
3.32 Authenticated registration 199
3.33 Authentication via public key cryptography 199
3.34 An example of the PGP trust 202
3.35 Format of an SSH packet 205

4.1 Binary Symmetric Channel (BSC) with error probability p 216
4.2 The EAN-128 code for foundations of coding 219
4.3 Example of a (10,5) regular LDPC code and its representation by a Tanner graph. The six bold edges show a length-6 cycle in the graph 241
4.4 Example of the bit-flipping decoding over the Hamming code (7,4) for the received word $y = 0011101$ when the codeword $c = 0011001$ has been transmitted. (a) Step 2: parity checks, (b) step 3: codeword update, and (c) stopping criteria (success) 244
4.5 Illustration of the extrinsic information passed to compute the messages $r_{j,i}^{(r)}$ (a, step 2) and $q_{i,j}^{(r)}$ (b, step 3) 246
4.6 25×25 QR-code and pattern locations 261
4.7 3-L, 29×29, QR-code for http://foundationsofcoding.imag.fr 262
4.8 State diagram of the convolutional code of generator polynomials $P_1 = X$ and $P_2 = X + 1$ 270
4.9 Lattice of the convolutional code generated by $P_1 = X$ and $P_2 = X + 1$ 271
4.10 Systematic convolutional code of constraint length 3 transformed into a RSC code 273
4.11 Parallel composition and interleaving of two RSC encoders 274
4.12 Iterative decoding of a turbo code 275

1 Encoding of a message M 278
2 Decoding of a message $M' = CORR(CRYPT(COMP(M)))$ 278
3 Viterbi's algorithm on the message 10010010011101111010 339

List of Tables

1.1 Letter Distribution in this LaTeX Script 12
1.2 Typical Complexity Bounds Obtained from an Algorithm Analysis 14
1.3 Extract of the ASCII Code 27
1.4 Zech's Construction on Invertible Elements in Odd Characteristic 54
1.5 Discrete Logarithm and Exponentiation in Finite Fields and Generic Groups 58
1.6 Group Laws in Characteristics 2 and 3 with $P = (x_1, y_1) \neq -P$ and $Q = (x_2, y_2) \neq \pm P$ 61
1.7 χ^2 Table (Extract) 67
1.8 Distribution of the Multiples of p Modulo m 90
1.9 Quadratic Sieve for 7429 94

2.1 Arithmetic Encoding of “bebecafdead” 110
2.2 Arithmetic Decoding of “0.15633504500” 111
2.3 Integer Arithmetic Encoding of “bebecafdead” 112
2.4 Integer Arithmetic Decoding of “156335043840” 113
2.5 Comparison of the Compression of an Email File (15.92 Mo: Text, Images, Programs, etc.) with Several Algorithms, on a PIV 1.5 GHz 126

3.1 Frequency of the Letters in French 142
3.2 Frequency Analysis of the Ciphertext 142
3.3 Rabbit Stream Internal State Evolution and Bit Extraction 144
3.4 Complexities of Cryptanalysis Methods on DES 150
3.5 Cost and Efficiency of Attacks on DES in 1996 150
3.6 Performance of Several Block Ciphers 152
3.7 Configurations for AES 153
3.8 Value of the Shift According to the Value of N_b in ShiftRows 156
3.9 Man-in-the-Middle Attack on the Diffie–Hellman Protocol 162
3.10 Sending of a Message Intercepted by the Man-in-the-Middle 162
3.11 Frequential Repartition of Symbols in a Text Written in French 171
3.12 Conjectured Compared Security of Block Ciphers 175
3.13 Main Differences between W and Rijndael 180
3.14 SHA-3 Candidates Speed (Cycles/Byte) on an Intel i7 180
3.15 Resistance to Collisions for the Most Famous Hash Functions 181

4.1 Order of Magnitude of Raw Error Rates 210
4.2 Encoding with a Parity Bit 212
4.3 Error Correction using Parity Bits 213
4.4 Examples of CRC Codes 223
4.5 Comparison of MPAs 246
4.6 Initial Interleaving Table with Delay 2 for Codewords of Length 5 264
4.7 Interleaving Table with Delay 2 After One Round 264

1 Several Primitive Polynomials in $\mathbb{F}_2[X]$ 279
2 Die Simulation by Coin Toss 296

List of Algorithms

1.1 Simplified Fax Encoding for a Line of Pixels 8
1.2 Fax Decoding for a Decrypted and Checked Line 10
1.3 GCD: Euclidean Algorithm 35
1.4 GCD: Extended Euclidean Algorithm 37
1.5 Modular Exponentiation 41
1.6 Miller–Rabin Primality Test 45
1.7 Horner Polynomial Evaluation 47
1.8 Ben-Or’s Irreducibility Test 50

1.9 Generation of a sparse irreducible polynomial 51
1.10 Test Primitive Root 55
1.11 Test Generator Polynomial 56
1.12 Discrete Fast Fourier Transform 82
1.13 Fast product of two polynomials 84
1.14 Berlekamp–Massey Algorithm 87
1.15 Yuval's birthday attack 89
1.16 Pollard's Factoring 91
1.17 Lenstra's elliptic curve factoring 92
1.18 Gordon's algorithm 95

2.1 Description of Huffman's Algorithm 104
2.2 Arithmetic Encoding 110
2.3 Arithmetic Decoding 111
2.4 Dynamic Huffman Algorithm: Compression 115
2.5 Dynamic Huffman's Algorithm Decompression 116
2.6 Inverse of BWT 122
2.7 Lempel-Ziv-Welch (LZW): compression 124
2.8 LZW: decompression 125

3.1 AES Encryption 154
3.2 Key Schedule in AES 159
3.3 Galois Counter Mode 186
3.4 Shamir's Trick for Simultaneous Double-And-Add 191

4.1 Hard-Decision Decoder by Bit-Flipping Algorithm 243
4.2 Generic Belief Propagation Algorithm for LDPC Code Decoding 245
4.3 Decoding of a Reed-Solomon code 259
4.4 Viterbi's Algorithm (Decoding of Convolutional Codes) 272

1 AES Decryption 308
2 Factoring n from (n,e,d) in RSA (Special Case: e is Small) 314
3 Factoring n from (n, e, d) in RSA 315
4 RSA Cryptographic Pseudo-Random Generator 319
5 Repetition Code Decoding with Maximum Detection 326
6 Repetition Code Decoding with Maximum Correction 327
7 Repetition Code Decoding with Detection and Correction 327
8 Minimum Distance of a Code ($|V| = 2$) 328

Acronyms

ADSL Asymmetric Digital Subscriber Line 276
AES Advanced Encryption Standard vi
AKS Agrawal–Kayal–Saxena 45

此为试读,需要完整PDF请访问: www.ertongbook.com