

Peter Seibt

# Algorithmic Information Theory

Mathematics of Digital Information  
Processing

With 14 Figures

 Springer

Peter Seibt  
Université de la Méditerranée  
and  
Centre de Physique Théorique  
Campus de Luminy, Case 907  
13288 Marseille cedex 9, France

Library of Congress Control Number: 2006925851

ISSN 1860-4862

ISBN-10 3-540-33218-9 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-33218-3 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media.

[springer.com](http://springer.com)

© Springer-Verlag Berlin Heidelberg 2006

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting by the authors and SPi

Cover design: Design & Production, Heidelberg

Printed on acid-free paper      SPIN: 11607311      62/2162/SPi      5 4 3 2 1 0

---

## Contents

<b>1</b>	<b>Data Compaction</b> .....	5
1.1	Entropy Coding .....	5
1.1.1	Discrete Sources and Their Entropy .....	5
1.1.2	Towards Huffman Coding .....	10
1.1.3	Arithmetic Coding .....	32
1.2	Universal Codes: The Example LZW .....	43
1.2.1	LZW Coding .....	43
1.2.2	The LZW Decoder .....	45
<b>2</b>	<b>Cryptography</b> .....	49
2.1	The Data Encryption Standard .....	50
2.1.1	The DES Scheme .....	50
2.1.2	The Cipher DES in Detail .....	53
2.2	The Advanced Encryption Standard: The Cipher Rijndael ....	60
2.2.1	Some Elementary Arithmetic .....	60
2.2.2	Specification of Rijndael .....	77
2.2.3	The Key Schedule .....	86
2.2.4	Decryption with Rijndael .....	92
2.3	The Public Key Paradigm and the Cryptosystem RSA .....	93
2.3.1	Encryption and Decryption via Exponentiation .....	93
2.3.2	The Cryptosystem RSA .....	97
2.4	Digital Signatures .....	101
2.4.1	Message Digests via SHA-1 .....	101
2.4.2	DSA: Digital Signature Algorithm .....	112
2.4.3	Auxiliary Algorithms for DSA .....	116
2.4.4	The Signature Algorithm rDSA .....	122
2.4.5	ECDSA – Elliptic Curve Digital Signatures .....	125
<b>3</b>	<b>Information Theory and Signal Theory: Sampling and Reconstruction</b> .....	171
3.1	The Discrete Fourier Transform .....	172

VI Contents

3.1.1	Basic Properties . . . . .	172
3.1.2	The Fast Fourier Transform Algorithm . . . . .	183
3.2	Trigonometric Interpolation . . . . .	190
3.2.1	Trigonometric Polynomials . . . . .	191
3.2.2	Sampling and Reconstruction . . . . .	193
3.3	The Whittaker–Shannon Theorem . . . . .	198
3.3.1	Fourier Series . . . . .	198
3.3.2	The Whittaker–Shannon Theorem for Elementary Periodic Functions . . . . .	203
3.3.3	The (Continuous) Fourier Transform: A Sketch . . . . .	209
3.3.4	The Sampling Theorem . . . . .	214
<b>4</b>	<b>Error Control Codes . . . . .</b>	<b>221</b>
4.1	The Reed–Solomon Codes . . . . .	221
4.1.1	Preliminaries: Polynomial Codes . . . . .	221
4.1.2	Reed–Solomon Codes . . . . .	225
4.2	Convolutional Codes . . . . .	239
4.2.1	Encoding: Digital Filtering in Binary Arithmetic . . . . .	239
4.2.2	Decoding: The Viterbi Method . . . . .	253
<b>5</b>	<b>Data Reduction: Lossy Compression . . . . .</b>	<b>267</b>
5.1	DFT, Passband Filtering and Digital Filtering . . . . .	268
5.2	The Discrete Cosine Transform . . . . .	274
5.2.1	Functional Description of the DCT . . . . .	275
5.2.2	The 2D DCT . . . . .	293
5.2.3	The Karhunen–Loève Transform and the DCT . . . . .	305
5.3	Filter Banks and Discrete Wavelet Transform . . . . .	314
5.3.1	Two Channel Filter Banks . . . . .	314
5.3.2	The Discrete Wavelet Transform . . . . .	372
	<b>References . . . . .</b>	<b>435</b>
	<b>Index . . . . .</b>	<b>439</b>