

Translations of

MATHEMATICAL MONOGRAPHS

Volume 203

Mathematics of Information and Coding

Te Sun Han
Kingo Kobayashi



American Mathematical Society

Selected Titles in This Series

- 203 **Te Sun Han and Kingo Kobayashi**, Mathematics of information and coding, 2002
- 202 **V. P. Maslov and G. A. Omel'yanov**, Geometric asymptotics for nonlinear PDE. I, 2001
- 201 **Shigeyuki Morita**, Geometry of differential forms, 2001
- 200 **V. V. Prasolov and V. M. Tikhomirov**, Geometry, 2001
- 199 **Shigeyuki Morita**, Geometry of characteristic classes, 2001
- 198 **V. A. Smirnov**, Simplicial and operad methods in algebraic topology, 2001
- 197 **Kenji Ueno**, Algebraic geometry 2: Sheaves and cohomology, 2001
- 196 **Yu. N. Lin'kov**, Asymptotic statistical methods for stochastic processes, 2001
- 195 **Minoru Wakimoto**, Infinite-dimensional Lie algebras, 2001
- 194 **Valery B. Nevzorov**, Records: Mathematical theory, 2001
- 193 **Toshio Nishino**, Function theory in several complex variables, 2001
- 192 **Yu. P. Solovyov and E. V. Troitsky**, C^* -algebras and elliptic operators in differential topology, 2001
- 191 **Shun-ichi Amari and Hiroshi Nagaoka**, Methods of information geometry, 2000
- 190 **Alexander N. Starkov**, Dynamical systems on homogeneous spaces, 2000
- 189 **Mitsuru Ikawa**, Hyperbolic partial differential equations and wave phenomena, 2000
- 188 **V. V. Buldygin and Yu. V. Kozachenko**, Metric characterization of random variables and random processes, 2000
- 187 **A. V. Fursikov**, Optimal control of distributed systems. Theory and applications, 2000
- 186 **Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito**, Number theory 1: Fermat's dream, 2000
- 185 **Kenji Ueno**, Algebraic Geometry 1: From algebraic varieties to schemes, 1999
- 184 **A. V. Mel'nikov**, Financial markets, 1999
- 183 **Hajime Sato**, Algebraic topology: an intuitive approach, 1999
- 182 **I. S. Krasil'shchik and A. M. Vinogradov, Editors**, Symmetries and conservation laws for differential equations of mathematical physics, 1999
- 181 **Ya. G. Berkovich and E. M. Zhmud'**, Characters of finite groups. Part 2, 1999
- 180 **A. A. Milyutin and N. P. Osmolovskii**, Calculus of variations and optimal control, 1998
- 179 **V. E. Voskresenskiĭ**, Algebraic groups and their birational invariants, 1998
- 178 **Mitsuo Morimoto**, Analytic functionals on the sphere, 1998
- 177 **Satoru Igari**, Real analysis—with an introduction to wavelet theory, 1998
- 176 **L. M. Lerman and Ya. L. Umanskiy**, Four-dimensional integrable Hamiltonian systems with simple singular points (topological aspects), 1998
- 175 **S. K. Godunov**, Modern aspects of linear algebra, 1998
- 174 **Ya-Zhe Chen and Lan-Cheng Wu**, Second order elliptic equations and elliptic systems, 1998
- 173 **Yu. A. Davydov, M. A. Lifshits, and N. V. Smorodina**, Local properties of distributions of stochastic functionals, 1998
- 172 **Ya. G. Berkovich and E. M. Zhmud'**, Characters of finite groups. Part 1, 1998
- 171 **E. M. Landis**, Second order equations of elliptic and parabolic type, 1998
- 170 **Viktor Prasolov and Yuri Solovyev**, Elliptic functions and elliptic integrals, 1997
- 169 **S. K. Godunov**, Ordinary differential equations with constant coefficient, 1997
- 168 **Junjiro Noguchi**, Introduction to complex analysis, 1998
- 167 **Masaya Yamaguti, Masayoshi Hata, and Jun Kigami**, Mathematics of fractals, 1997
- 166 **Kenji Ueno**, An introduction to algebraic geometry, 1997

(Continued in the back of this publication)

This page intentionally left blank

Mathematics of Information and Coding

This page intentionally left blank

Translations of
**MATHEMATICAL
MONOGRAPHS**

Volume 203

**Mathematics of
Information and
Coding**

Te Sun Han
Kingo Kobayashi



American Mathematical Society
Providence, Rhode Island

Editorial Board

Shoshichi Kobayashi (Chair)
Masamichi Takesaki

MATHEMATICS OF INFORMATION AND CODING

by Te Sun Han and Kingo Kobayashi

Copyright © 1994 by Te Sun Han and Kingo Kobayashi

Originally published in Japanese by Iwanami Shoten, Publishers, Tokyo in 1994

Translated from the Japanese by Joe Suzuki

2000 *Mathematics Subject Classification*. Primary 00A69, 94–02, 94A24, 94A29, 94A15,
94A45, 68P30, 62F03, 62F12.

Library of Congress Cataloging-in-Publication Data

Han, Te Sun, 1941–

[Joho to fugoka no suri. English]

Mathematics of information and coding / Te Sun Han, Kingo Kobayashi.

p. cm. — (Translations of mathematical monographs ; v. 203)

ISBN 0-8218-0534-7 (hard cover; alk. paper)

ISBN 0-8218-4256-0 (soft cover; alk. paper)

1. Coding theory. 2. Information theory. I. Kobayashi, Kingo, 1943– II. Title. III. Series.

QA268.H355 2002
003'.54—dc21

2001041262

Copying and reprinting. Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to reprint-permission@ams.org.

© 2002 by the American Mathematical Society. All rights reserved.

Reprinted by the American Mathematical Society, 2007.

The American Mathematical Society retains all rights
except those granted to the United States Government.

Printed in the United States of America.

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.

Visit the AMS home page at <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 12 11 10 09 08 07

Dedicated to Claude E. Shannon

Research rather than exposition is the keynote.
— Claude E. Shannon

This page intentionally left blank

Contents

Preface to the English Edition	xi
Chapter 1. What is Information Theory?	1
1.1. Introduction	1
1.2. Information Theory So Far	2
1.3. Basic Elements and Related Fields	6
1.4. About this Book	16
Chapter 2. Basics of Information Theory	19
2.1. Entropy	19
2.2. Divergence	25
2.3. Mutual Information	31
2.4. Data Processing Inequality	37
2.5. Fano's Inequality	40
2.6. Type of Sequences, Typical Sequences, and AEP	41
Exercises	51
Chapter 3. Source and Coding	73
3.1. Various Information Sources	73
3.2. Entropy Rate of Source	79
3.3. Various Codes	84
3.4. AEP and Source Coding Theorem	86
3.5. Separable Codes and Prefix Codes	88
3.6. Converse Theorem for FV Coding	93
3.7. Direct Theorem for FV Coding	95
3.8. Huffman Code	99
3.9. Coding for Arbitrarily Varying Sources	106
3.10. Reliability Function for Source Coding	109
Exercises	115
Chapter 4. Arithmetic Code	127
4.1. Elias Code	127
4.2. Algorithm of Arithmetic Code	131
4.3. Asymptotic Optimality of Arithmetic Code	139
4.4. Arithmetic Code as Number System	142
4.5. Enumerative Code	145
4.6. Arithmetic Code as Tree Code	148
Exercises	151
Chapter 5. Universal Coding of Integers	157
5.1. Universal Codes of Integers	157

5.2. Search Tree of Bentley-Yao	166
5.3. Bounds for Elias Codeword Length Functions	170
5.4. Properties of the Log-Star Function	180
5.5. Modified Log-Star Functions	182
Exercises	188
Chapter 6. Universal Coding of Texts	193
6.1. Lempel-Ziv Code based on Incremental Parsing	193
6.2. Lempel-Ziv Code based on Recurrence Time	202
Exercises	214
Chapter 7. Universal Coding of Compound Sources	219
7.1. Compound Source	219
7.2. Sub-Probability and Codeword Length	220
7.3. Universal Code for Compound Source	222
7.4. Estimation of Probability Distribution	223
7.5. Rissanen's Two-Step Coding	225
7.6. Rissanen's Predictive Coding	231
7.7. Stochastic Complexity	233
7.8. Bayes Code	234
7.9. Model Selection and Universal Code	239
7.10. Consistency of Model Selection	242
Exercises	248
Chapter 8. Data Analysis and MDL Principle	253
8.1. Fitting of Experimental Data	254
8.2. Histogram Approximation for Probability Density	257
8.3. Self-Organization of Data	258
8.4. Self-Formation of Category	262
8.5. Category Classification by Decision Tree	263
8.6. Probabilistic Category Classification	266
8.7. About AIC Criterion	269
Exercises	273
Bibliography	277
Index	283

Preface to the English Edition

This book is intended to provide engineering and/or statistic students, communication engineers, and relevant mathematicians with a firm theoretic basis in *source coding* (or *data compression*) in information theory. Usually, standard information theory textbooks contain not only *source coding* but also *channel coding*. In this book, however, we have focused only on *source coding*. The reason is first that *source coding* is generally more basic than *channel coding* in elementary information theory textbooks, and second that the advancement of theories and practices in source coding has indeed been prominent, particularly in the 1990's, and so we have preferred to systematically describe this recent advancement of source coding from the very basics to the top frontiers in an intuitively transparent but mathematically sound manner. We believe that this systematic manner is possibly one of the best methods to help the reader clearly and deeply understand step-by-step the probabilistic and/or combinatorial essences of *source coding*.

As a consequence, however, we regret that we have no space to discuss *channel coding*. We just hope to be fortunate enough to have an opportunity in the near future to write another book about *channel coding*.

The main modern trend of source coding is featured by the *universality* of coding schemes, where by universality we mean that an encoder and a decoder can achieve the asymptotically optimal compression ratio without even knowing the source statistic. In view of this trend, we have attempted as much as possible in this book to highlight the *universality*.

This book consists of eight chapters. Chapter 1 provides a short overview about several typical areas in the very wide spectrum of information theory. This chapter will enable the reader to intuitively grasp what information theory is to deal with. Chapters 2 and 3 are devoted to the basic notions of information theory and the fundamental mechanism of source coding, respectively. By reading only these three chapters, the reader could obtain clear insight into the fundamental notions of information theory. We give a comprehensive description of *arithmetic code* in Chapter 4. Although arithmetic code itself is *not* originally universal, it is straightforward to modify the original version of arithmetic code so as to be *universal*. In fact, various kinds of universal codes in this direction have actually been devised. Chapters 5, 6, and 7 are devoted to *universal coding* of integers, *universal coding* of texts, and *universal coding* of compound sources, respectively. These three chapters elucidate, from a respective point of view, the relevant theoretical details of the modern and standard *universal codings*. Finally, Chapter 8 is incorporated to demonstrate that the universal coding as stated in Chapter 7 is directly applicable, as a general principle (called the MDL principle), also to a wide range of data analysis problems, including problems of pattern recognition, self-organization of data, machine learning, artificial intelligence, and so on.

Thus, this book can be said to be an attempt to summarize as compactly as possible a modern typical trend of universal source codings as well as its applications to statistical data analysis in general. This clearly reveals a new intrinsic linkage between information theory and statistics, although these two research fields have been regarded for a long time as being separate.

Furthermore, in this English version, at the end of each chapter (except for Chapter 1), a considerable number of exercises are appended (approximately 60 pages in total). This will help the reader not only to understand more deeply the essence of those arguments as developed in the text, but also to broaden their own views about the many interesting information-theoretic topics. The reader may enjoy reading and proving these exercises.

We would like to thank all the people who, in one way or another, helped us publish this book. First, we should thank Masao Iri and Shun-ichi Amari who gave us the chance to write this book. We are grateful also to Suguru Arimoto who stimulated our fascination with information theory. Our sincere gratitude goes also to our colleagues Shojiro Sakata, Mamoru Hoshi, and Hiroyoshi Morita for useful discussions. We are very thankful to Joe Suzuki who prepared the first English draft of this book, without which the present English version could not have appeared. Last, we would like to thank all members of I&C (a small research group for Information and Coding in Tokyo). In particular, we are very pleased to thank Hiroshi Sato who not only organized this group but has continued to take the leading role in research activities at I&C.

Te Sun Han
Kingo Kobayashi
April 24, 2001

Bibliography

General References

1. N. Abramson, *Information Theory and Coding*, McGraw-Hill Inc., New York, 1963.
2. P. Billingsley, *Ergodic Theory and Information*, John Wiley & Sons, New York, 1965.
3. R. E. Blahut, *Principles and Practice of Information Theory*, Addison-Wesley, Tokyo, 1987.
4. R. E. Blahut, *Digital Transmission of Information*, Addison-Wesley, 1990.
5. L. Brillouin, *Science and Information Theory*, 2nd ed., Academic Press, New York, 1962.
6. Thomas M. Cover, P. Gacs and R. M. Gray, Kolmogorov's contributions to information theory and algorithmic complexity, *Annals of Probability*, vol.17, 840-865, 1989.
7. Thomas M. Cover and Joy A. Thomas, *Elements of Information Theory*, John Wiley & Sons, New York, 1991.
8. Imre Csiszár and Janos Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York, 1981.
9. W. Feller, *An Introduction to Probability Theory and its Applications*, vol. 2, 2nd ed., John Wiley & Sons, New York, 1971.
10. R. G. Gallager, *Information Theory and Reliable Communication*, Wiley, New York, 1968.
11. F. Jelinek, *Probabilistic Information Theory*, McGraw-Hill, New York, 1968.
12. J. C. Kieffer, A survey of the theory of source coding with a fidelity criterion, *IEEE Transactions on Information Theory*, vol.IT-39, no.5, 1473-1490, 1993.
13. D. E. Knuth, *The Art of Computer Programming, Vol.III: Searching and Sorting*, Addison-Wesley, Reading, MA, 1973.
14. D. E. Knuth and A. C. Yao, The complexity of nonuniform random number generation, *Algorithms and Complexity: New Direction and Recent Results*, 357-428, ed. by J. F. Traub, Academic Press, New York, 1976.
15. R. J. McEliece, *The Theory of Information and Coding*, Addison-Wesley, Reading, MA, 1977.
16. J. Stoyanov, *Counter Examples in Probability*, John Wiley & Sons, New York, 1987.
17. J. Wolfowitz, *Coding Theorems of Information Theory*, 3rd ed., Springer-Verlag, New York, 1978.

Chapter 1

18. R. Ahlswede, A bad code are good cyphers, *Problems of Control and Information Theory*, vol.11, no.5, 337-351, 1982.
19. R. Ahlswede and I. Csiszár, Common randomness in information theory and cryptography, Part I: Secrecy sharing, *IEEE Transactions on Information Theory*, vol.IT-39, no.4, 1121-1132, 1993.
20. U. Maurer, Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory*, vol.IT-39, no.3, 733-742, 1993.
21. A. Barron and T. M. Cover, A bound on the financial value of information, *IEEE Transactions on Information Theory*, vol.IT-34, no.5, 1097-1100, 1988.
22. R. Bell and T. M. Cover, Competitive optimality of logarithmic investment, *Mathematics of Operations Research*, vol.5, 161-166, 1980.
23. T. Berger, *Rate Distortion Theory: A Mathematical Basis for Data Compression*, Prentice Hall, Englewood Cliffs, NJ, 1971.

24. G. J. Chaitin, Information-theoretic computational complexity, *IEEE Transactions on Information Theory*, vol.IT-20, no.1, 10–15, 1974.
25. G. J. Chaitin, A theory of program size formally identical to information theory, *J. Assoc. Comp. Mach.*, vol.22, 329–340, 1975.
26. G. J. Chaitin, Algorithmic information theory, *IBM J. Res. & Dev.*, vol.21, 350–359, 1977.
27. T. M. Cover, Universal portfolios, *Mathematical Finance*, vol.16, 876–898, 1991.
28. El Gamal and T. M. Cover, Multi user information theory, *Proceedings of IEEE*, vol.68, 1466–1483, 1980.
29. R. M. Fano, *Transmission of Information: A Statistical Theory of Communication*, Wiley, New York, 1961.
30. A. Feinstein, *Foundations of Information Theory*, McGraw-Hill, New York, 1958.
31. B. Marcus, Sofic systems and encoding data, *IEEE Transactions on Information Theory*, vol.IT-31, no.3, 366–377, 1985.
32. D. Lind and B. Marcus, *An Introduction to Symbolic Dynamics and Coding*, Cambridge University Press, 1995.
33. K. Marton, Error exponent for source coding with a fidelity criterion, *IEEE Transactions on Information Theory*, vol.IT-20, no.2, 197–199, 1974.
34. A. Sgarro, Error probabilities for simple substitution ciphers, *IEEE Transactions on Information Theory*, vol.IT-29, no.2, 190–198, 1983.
35. G. Ungerboeck, Trellis coding with expanded channel signal sets, *Proceedings of IEEE International Symposium on Information Theory*, Ithaca, 1977.
36. A. D. Wyner, The wire-tap channel, *Bell System Technical Journal*, vol.54, 1355–1387, 1975.
37. I. Csiszár and J. Körner, Broadcast channels with confidential messages, *IEEE Transactions on Information Theory*, vol.IT-24, no.3, 339–348, 1978.

Chapter 2

38. C. H. Bennett, Demons, engines and the second Law, *Scientific American*, vol. 295(5), 108–116, 1987.
39. S. Verdú and T. S. Han, A general formula for channel capacity, *IEEE Transactions on Information Theory*, vol.IT-40, no.3, 1147–1157, 1994.
40. T. S. Han and S. Verdú, Approximation theory of output statistics, *IEEE Transactions on Information Theory*, vol.IT-39, no.3, 752–772, 1993.
41. Thomas M. Cover and Joy A. Thomas, *Elements of Information Theory*, John Wiley & Sons, New York, 1991.
42. Imre Csiszár and Janos Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York, 1981.

Chapter 3

43. P. Algoet and T. M. Cover, A sandwich proof of the Shannon-McMillan-Breiman theorem, *Annals of Probability*, vol.16, 899–909, 1988.
44. R. B. Ash, *Information Theory*, John Wiley & Sons, Interscience, New York, 1965.
45. L. Breiman, The individual ergodic theorem of information theory, *Ann. Math. Stat.*, vol.28, no.3, 809–811, 1957.
46. L. Breiman, Correction to the individual ergodic theorem of information theory, *Ann. Math. Stat.*, vol.31, no.3, 809–810, 1960.
47. J. A. Bucklew, *Large Deviation Techniques in Decision, Simulation and Estimation*, John Wiley & Sons, New York, 1991.
48. J. A. Fill, Asymptotic expansions for large deviation probabilities in the strong law of large numbers, *Probability Theory and Related Fields*, vol.81, 213–233, 1989.
49. P. Walters, *Ergodic Theory—Introductory Lectures*, Lecture Notes in Mathematics, no.458, Springer-Verlag, New York, 1975.
50. S. Verdú and T. S. Han, The role of the asymptotic equipartition property in noiseless source coding, *IEEE Transactions on Information Theory*, vol.IT-43, no.3, 847–857, 1997.

Chapter 4

51. M. Guazzo, A general minimum-redundancy source coding algorithm, *IEEE Transactions on Information Theory*, vol.IT-26, no.1, 15–25, 1980.
52. T. S. Han, Recent Progress of Data Compression Theory, I, II (in Japanese), *Journal of IEICE*, vol. 67, no. 2:185–191, no. 3:286–292, 1984.
53. C. B. Jones, An efficient coding system for long source sequences, *IEEE Transactions on Information Theory*, vol.IT-27, no.3, 280–291, 1981.
54. G. G. Langdon, An introduction to arithmetic coding, *IBM J. Res. & Dev.*, vol.28, 135–149, 1984.
55. J. Rissanen, Modeling by shortest data description, *Automatica*, vol.14, 465–471, 1978.
56. J. Rissanen, Arithmetic coding as number representation, *Acta Polyt. Scandinavica*, 44–51, Dec. 1979.
57. J. Rissanen and G. G. Langdon, Arithmetic coding, *IBM J. Res. & Dev.*, vol.23, 149–169, 1979.
58. J. Rissanen and G. G. Langdon, Universal coding and modeling, *IEEE Transactions on Information Theory*, vol.IT-27, no.1, 12–22, 1981.
59. H. Suzuki, H. Sato and K. Kobayashi, Arithmetic coding realizing arbitrary output distributions (in Japanese), *Proc. of the Seventh Symposium on Information Theory and its Applications*, 580–585, 1984.

Chapter 5

60. L. D. Davisson, Universal noiseless coding, *IEEE Transactions on Information Theory*, vol.IT-19, no.6, 783–795, 1973.
61. S. Even and M. Radeh, Economical encoding of commas between strings, *Technion Tech. Rep.*, no.54, Haifa, Israel, 1975.
62. J. Rissanen, A universal prior for integers and estimation by minimum description length, *Annals of Statistics*, vol.11, 416–431, 1983.
63. Q. F. Stout, Improved prefix encodings of the natural numbers, *IEEE Transactions on Information Theory*, vol.IT-26, no.5, 607–609, 1980.
64. Q. F. Stout, Searching and encoding for infinite ordered set, *International Journal of Computer and Information Sciences*, vol.11, 55–72, 1982.
65. V. I. Levenshtein, On the redundancy and delay of decodable coding of natural numbers (in Russian), *Problems of Cybernetics*, vol.20, 173–179, 1968.

Chapter 6

66. R. S. Boyer and J. S. Moore, A fast string searching algorithm, *Commun. ACM*, vol.20, 10, 762–772, 1977.
67. P. E. Bender and J. K. Wolf, New asymptotic bounds and improvements on the Ziv-Lempel data compression algorithm, *IEEE Transactions on Information Theory*, vol.IT-37, no.3, 721–729, 1991.
68. N. Faller, An adaptive system for data compression, *Record of the 7-th Asilomar Conference on Circuits, Systems and Computers*, 593–597, 1973.
69. T. S. Han, Recent Progress of Data Compression Theory, I, II (in Japanese), *Journal of IEICE*, vol. 67, no. 2:185–191, no. 3:286–292, 1984.
70. H. Yokoo, Recent techniques of adaptive data compression (in Japanese), *Computer Vision*, vol. 90-3, 17–24, 1994.
71. H. Yamamoto, Universal data compression algorithm: principle and method (in Japanese), *Information Processing*, vol.135, no.7, 600–608, 1994.
72. M. Kac, On the notion of recurrence in discrete stochastic process, *Bull. American Mathematical Society*, vol.53, 1002–1010, 1947.
73. R. M. Karp and M. O. Rabin, Efficient randomized pattern-matching algorithms, *Technical Report TR-31-81*, Aiken Comput. Lab., Harvard University, Cambridge, MA, 1981.

74. J. C. Kieffer, Sample converses in source coding theory, *IEEE Transactions on Information Theory*, vol.IT-37, no.2, 263–268,1991.
75. D. E. Knuth, Dynamic Huffman coding, *J. Algorithms*, vol. 6, 163–180, 1985.
76. D. E. Knuth, J. H. Morris and V. R. Pratt, Fast pattern matching in string, *SIAM Journal on Computing*, vol.6, no.2, 323–350, 1977.
77. G. G. Langdon, A note on the Lempel-Ziv model for compressing individual sequences, *IEEE Transactions on Information Theory*, vol.IT-29, no. 2, 284–287, 1983.
78. D. S. Ornstein and P. C. Shields, Universal almost sure data compression, *Annals of Probability*, vol.18, 441–452, 1990.
79. J. S. Vitter, Design and Analysis of Dynamic Huffman Codes, *J. of ACM*, vol. 34, no.4, 825–845, 1987.
80. M. J. Weinberg, A. Lempel and J. Ziv, A sequential algorithm for the universal coding of finite memory sources, *IEEE Transactions on Information Theory*, vol.IT-38, no.3, 1002–1014, 1992.

Chapter 7

81. A. Barron and T. M. Cover, Minimum complexity density estimation, *IEEE Transactions on Information Theory*, vol. IT-37, no.4, 1034–1054, 1991.
82. D. Blackwell and M. A. Girshick, *Theory of Games and Statistical Decisions*, John Wiley & Sons, London, 1954.
83. B. S. Clarke and A. R. Barron, Jeffreys prior is asymptotically least favorable under entropy risk, *Journal of Statistical Planning and Inference*, vol.41, no.1, 37–61, 1994.
84. L. D. Davission, Minimax noiseless universal coding for Markov sources, *IEEE Transactions on Information Theory*, vol.IT-29, no.2, 211–215. 1983.
85. L. Györfi, I. Pali and E. C. van der Meulen, On universal noiseless source coding for infinite source alphabets, *European Transactions on Telecommunications and Related Technologies*, vol.4, 17–24, March-April, 1993.
86. L. Györfi, I. Pali and E. C. van der Meulen, There is no universal source code for infinite source alphabet, *IEEE Transactions on Information Theory*, vol.IT-40, no.1, 267–271, 1994.
87. S. Karlin, *Mathematical Methods and Theory in Games*, Programming and Economics, Addison-Wesley, Reading, MA, 1959.
88. N. Merhav, M. Gutman and J. Ziv, On the estimation of the order of a Markov chain and universal data compression, *IEEE Transactions on Information Theory*, vol.IT-35, no.5, 1014–1019, 1989.
89. J. Rissanen, A universal data compression system, *IEEE Transactions on Information Theory*, vol.IT-29, no.5, 656–664, 1983.
90. J. Rissanen, Universal coding, information, prediction and estimation, *IEEE Transactions on Information Theory*. vol.IT-30, no.4, 629–636, 1984.
91. J. Rissanen, Complexity of strings in the class of Markov sources, *IEEE Transactions on Information Theory*, vol.IT-32, no.4, 526–532, 1986.
92. J. Rissanen, Stochastic complexity and modeling, *Annals of Statistics*, vol.14, no.3, 1080–1100, 1986.
93. J. Rissanen, Stochastic complexity, *J. R. Statist. Soc. B*, vol.49, no.3, 223–239 and 252–265, 1987.
94. G. Schwarz, Estimating the dimension of a model, *Annals of Statistics*, vol.6, 461–464, 1978.
95. J. Ziv and N. Merhav, Estimating the number of states of a finite-state source, *IEEE Transactions on Information Theory*, vol.IT-38, no.1, 61–65, 1992.

Chapter 8

96. S. Itoh, Application of the MDL principle to pattern recognition (in Japanese), *Journal of JSAI*, vol. 7, no. 4, 608–614, 1992.
97. J. Rissanen, A universal prior for integers and estimation by minimum description length, *Annals of Statistics*, vol.11, 416–431, 1983.

98. J. Rissanen and B. Yu, MDL learning, *Learning and Geometry: Computational Approaches*, ed. by D. W. Kueker and C. H. Smith, Birkhauser, 3–10, Boston, 1996.
99. G. Schwarz, Estimating the dimension of a model, *Annals of Statistics*, vol.6, 461–464, 1978.
100. K. Yamanishi and T. S. Han, Introduction to MDL: from the information theoretic point of view (in Japanese), *Journal of JSAI*, vol. 7, no. 3, 427–434, 1992.
101. J. Ziv, On the classification with empirically observed statistics and universal data compression, *IEEE Transactions on Information Theory*, vol.IT-34, no.2, 278–286, 1988.
102. R. L. Quinlan and R. Rivest, Inferring decision trees using the minimum description principle, *Information and Computation*, vol.80, 227–248, 1989.
103. K. Akaike, A new look at the statistical model identification, *IEEE Transactions on Automatic Control*, vol.AC-19, 716–723, 1974.
104. K. Akaike, What is the information criterion AIC?— its meaning and prospect to the future (in Japanese), *Mathematical Science*, no.153, 5–11, Science-sha, 1976.
105. K. Takeuchi, The distribution of information statistics and criterion of adequateness of models (in Japanese), *Mathematical Science*, no.153, 12–18, Science-sha, 1976.
106. R. Shibata, Asymptotically efficient selection of the order of the model for estimating parameters of a linear process, *Annals of Statistics*, vol.8, 147–164, 1980.
107. R. Shibata, An optimal selection of regression variables, *Biometrika*, vol.68, 45–54, 1981.
108. R. Shibata, Statistical inference and model selection (in Japanese), *Mathematical Science*, no.213, 45–50, Science-sha, 1981.
109. K. Nagaoka, Y. Kikuchi and K. Ikeda, On the consistency of model selection and prediction errors: comparing AIC and MDL (in Japanese), *Proc. of the Fifteenth Symposium on Information Theory and its Applications*, 369–372, Minakami, Japan, 1992.

This page intentionally left blank

Index

- (+1)-flat, 64
- (+1)-flat surface, 64
- (+1)-geodesic, 60, 61

- acceptance region, 62
- additivity
 - of divergence, 28
 - of entropy, 22
 - of mutual information, 34
- AEP
 - asymptotic equipartition property, 49
 - for general source, 121
 - for stationary ergodic source, 80
 - for stationary memoryless source, 49
- AIC, 269
- alphabet
 - code \sim , 85
 - continuous \sim , 19
 - discrete \sim , 19
 - finite \sim , 19
 - input \sim , 21
 - output \sim , 21
 - source \sim , 73
- ancestor, 103
- axiomatic information theory, 20

- Bayes decision problem, 264
- Bayes estimation, 58, 71
- binary entropy function, 21
- Birkhoff-von Neumann, 70
- bit, 20

- capacity
 - channel \sim , 3
 - noiseless channel \sim , 77
- category, 262
- chain rule, 23, 29
 - of divergence, 28
 - of entropy, 22
 - of mutual information, 34
- channel, 6, 21
 - \sim capacity, 3
 - \sim coding, 7
 - \sim with input constraints, 11
 - joint source- \sim coding, 7
 - memoryless \sim , 36
 - multiterminal \sim , 8

- Chebyshev inequality, 52
- Chernoff, 63
- Chernoff α -distance, 59
- Chernoff bound, 52
- Chernoff distance, 60
- child, 103
- co-polymatroid, 56
- code, 84
 - \sim of pointer type, 202
 - \sim tree, 92
 - \sim with constraint, 120
 - \sim with cost, 119
 - n -th extension of \sim , 88
- adaptive arithmetic \sim , 142, 214
- alphabetic \sim , 98
- arithmetic \sim , 5, 127, 131, 216
- asymptotically optimal universal \sim , 159
- Bayes \sim , 235
- block \sim , 85
- convolutional \sim , 86
- data translation \sim , 77
- dynamic Huffman \sim , 213
- Elias \sim , 129
- enumerative \sim , 145
- FF \sim , 85
- fixed-length \sim , 85
- FV \sim , 85
- Huffman \sim , 96
- instantaneous \sim , 89
- Lynch-Davisson \sim , 148
- LZ \sim , 216
- LZW \sim , 215
- min-max \sim , 238
- ω \sim , 162
- ω^* \sim , 163
- one-pass universal \sim , 142
- optimum prefix \sim , 100
- order-preserving \sim , 98, 144
- Pasco \sim , 138
- Pasco's FV \sim , 151
- Pasco's VF \sim , 152
- predictive \sim , 142
- prefix \sim , 89
- regular \sim , 88
- robust \sim , 78
- separable \sim , 88

- sequential \sim , 85, 137
- Shannon \sim , 95
- Shannon-Fano \sim , 95
- Shannon-Fano-Elias \sim , 96
- sliding block \sim , 86
- Stout \sim , 190
- synchronous \sim , 189
- translation \sim , 11
- tree \sim , 149
- two-pass Huffman \sim , 213
- unary \sim , 160
- uniquely decodable \sim , 88
- universal \sim , 10, 78, 111
- universally redundancy-bounded \sim , 159
- variable-length \sim , 85
- VF \sim , 85, 119
- VV \sim , 85
- codeword, 85
- codeword length
 - ideal \sim , 221
- coding
 - \sim of complete p -ary tree, 248
 - \sim rate, 86
 - \sim with cost, 153
 - channel \sim , 7
 - FF \sim , 123
 - FV \sim , 215
 - generalization of predictive \sim , 242
 - infinite Huffman \sim , 124
 - joint source-channel \sim , 7
 - predictive arithmetic \sim , 231, 252
 - Rissanen's two-step \sim , 225
 - source \sim , 7
 - source \sim theorem, 86
 - strongly universal \sim , 223
 - universal \sim , 5
 - VV \sim , 215
 - weakly universal \sim , 223
- compatibility, 74
- complete, 100
- complexity, 10, 193
- compression rate, 7
- concave, 23
 - concavity, 23
 - strictly \sim , 23
- conditional codeword length, 263
- conditional distribution, 263
- conditional division ratio, 135
 - accumulative \sim , 136, 138, 152
- consistency
 - of model estimation, 242
 - of model selection, 245
- constraint length, 86
- context gathering tree, 216
- conventional cryptography, 13
- converge in probability, 206
- converse theorem, 119, 154
- convex, 23
 - strictly \sim , 23
- convex closure, 106
- cost, 57, 145
- Cover, 56
- cryptography, 13
- Csiszár, 67
- Csiszár-Körner, 52
- cumulant, 64
- data compaction, 84
- data compression, 12, 84
- data protection, 13
- decision tree, 264
- decoder, 7, 84
- decoding, 7, 84
- decoding algorithm
 - of Pasco's FV code, 139
 - of Pasco's VF code, 152
- descendant, 103
- digit, 20
- direct theorem, 119, 154
- divergence, 12, 25, 56, 250
 - conditional \sim , 28
- empirical distribution, 42
- encoder, 7, 84
- encoding, 7, 84
- encoding algorithm
 - of Pasco's FV code, 138
 - of Pasco's VF code, 152
- ensemble average, 75
- entropy, 3, 7, 19, 20, 56, 117
 - \sim rate, 79
 - Boltzmann relative \sim , 25
 - conditional \sim , 4, 22
 - joint \sim , 21
 - of a type, 122
 - of random walk, 122
 - Renyi α - \sim , 59
 - Renyi \sim , 60
 - self- \sim , 20
 - topological \sim , 77
- ergodic decomposition, 75
- ergodic theorem
 - individual \sim , 75
 - pointwise \sim , 75
- error probability
 - decoding \sim , 109
 - of the first kind, 62
 - of the second kind, 62
- exponential family, 61, 64
- Fano's inequality, 40
- Fano-Horibe, 118
- finite memory, 77
- Fisher information matrix, 227, 249, 250
- flat-top, 121
- frequency sharing principle, 8
- Fujishige, 55

- Gallager-van Voorhis, 124
- gambling, 12
- general position, 65
- general source, 121
- generalized Chernoff distance, 66
- hidden Markov source, 116
- histogram density, 257
- Horibe, 54
- Hu's inequality, 58
- hypothesis testing, 62
- inconsistency, 269
- incremental parsing, 194
- information-spectrum, 80
- input block, 85
- Jeffreys' prior, 239
- Jensen's inequality, 23
- Kac's lemma, 203
- KC-complexity, 10, 233
- Kraft inequality, 89
- Kullback-Leibler information, 25
- Laplace estimator, 250, 252
- Laplace's asymptotic expansion, 235
- Laplace's principle of no reason, 180
- leaf, 91
- learning
 - with teacher, 268
 - without teacher, 268
- letter, 73
- Leung-Cover, 189
- level, 91
- likelihood function
 - generalized maximum logarithm \sim , 230
 - maximum logarithmic \sim , 230
- log-star function, 171
 - modified \sim , 182
- log-sum inequality, 25
- loss function, 225
- LZ complexity, 193
- majorize, 69
- Markov chain
 - k -th order \sim , 76
 - homogeneous \sim , 75, 76
 - irreducible homogeneous \sim , 76
 - simple \sim , 34
- Markov inequality, 51
- Markov inverse inequality, 52
- Massey, 53, 55, 121
- maximum entropy principle, 57
- MDL
 - \sim criterion, 254
 - \sim principle, 254
- memory coding problem, 120
- min-max redundancy, 238
- minimax theorem, 67, 237
- mixture, 235
- model
 - source \sim , 220
- model dimension, 220
- model selection, 253
- move-to-front, 213
- multi-user information theory, 4
- multiterminal information theory, 4
- mutual information, 7, 31
 - self- \sim , 33
- nat, 20
- nesting models, 246
- Neyman-Pearson, 62
- node, 91
- one-pass scheme, 213
- optimal, 62
- ordered tree, 118
- output block, 85
- $(p_0, p_1, \dots, p_{L-1})$ -ary representation, 143
- parametric compound source, 220
- parametric probability model, 220
- parent, 103
- pay-off, 237
- Pinsker's inequality, 57
- polymatroid, 55
- prediction distribution, 71
- prediction probability, 250
- predictive arithmetic coding, 216
- prefix, 89
- prefix code tree, 118
- prior, 235
- prior probability distribution, 241
- probability of correct decoding, 111
- public key cryptography, 13
- Pythagorean theorem, 30
 - of the first kind, 62
 - of the second kind, 68
- R-complexity, 233
- Rajski, 54
- random number generator, 123
- rate, 7
 - achievable \sim , 87
 - coding \sim , 86
 - entropy \sim , 79
- rate-distortion
 - \sim function, 20
 - \sim theory, 11
- recency rank, 213
- record, 166
- recurrence time, 203, 215
- redundancy, 223
- reliability function, 109
- Renyi α -entropy, 59
- Renyi entropy, 60
- repetition time, 203

- representative, 149
- root, 91
- RSA cryptography, 14
- Sanov's theorem, 124
- Sardinas-Patterson, 115
- saturated, 100
- search tree, 118, 166
 - binary \sim , 166
 - recurrence structure of \sim , 191
 - ultimate \sim , 167
- separation principle, 8
- Shannon, 53, 71
 - the first theorem of \sim , 86
- sibling, 103
 - \sim property, 104
- signal detection problem, 15
- signal estimation problem, 15
- Slepian-Wolf, 56
- source, 6
 - \sim alphabet, 73
 - \sim coding, 7
 - \sim coding theorem, 86
 - \sim model, 220
 - k -th order Markov \sim , 77
 - arbitrarily varying \sim , 78
 - compound \sim , 78
 - continuous \sim , 73
 - continuous time \sim , 73
 - discrete \sim , 73
 - discrete time \sim , 73
 - ergodic \sim , 75
 - finite state \sim , 77
 - hidden Markov \sim , 77
 - i.i.d. \sim , 78
 - information \sim , 73
 - joint \sim -channel coding, 7
 - Markov \sim , 76
 - Markov \sim in the broad sense, 77
 - mixed \sim , 79
 - multiterminal \sim , 8
 - nonparametric compound \sim , 220
 - nonstationary memoryless \sim , 78
 - stationary \sim , 74
 - stationary ergodic \sim , 75
 - stationary independent \sim , 78
 - stationary memoryless \sim , 43, 78
 - strongly entropic \sim , 121
 - unifilar \sim , 77
 - vector \sim , 73
- state, 75
- stationarity, 74
- stationary distribution, 76
 - k -th order \sim , 76
- stochastic complexity, 233
- stochastic matrix, 69
 - doubly \sim , 69
- stochastic process, 74
- stopping time, 119
- strong converse theorem, 87
- strongly consistent estimator, 225
- sub-probability, 221
- super-additivity, 132
- symbol, 73
- symbolic dynamics, 11, 77
- the second law in thermodynamics, 70
- time average, 75
- time sharing principle, 8
- transition probability
 - \sim matrix, 75
 - k -th order \sim , 76
- transmission rate, 7
- tree, 117
 - K -ary \sim , 91
 - code \sim , 92
 - complete \sim , 100
 - complete p -ary \sim , 248
 - context gathering \sim , 216
 - decision \sim , 264
 - ordered \sim , 118
 - prefix code \sim , 118
 - search \sim , 118
- triangle inequality, 53
- two-pass, 231
- type, 42
 - joint \sim , 43
- typical
 - \sim sequence, 46
 - ϵ - \sim , 47, 48
 - conditional \sim sequence, 50
 - conditional strongly ϵ - \sim , 50
 - jointly strongly ϵ - \sim , 50
 - strongly ϵ - \sim , 47
 - weakly ϵ - \sim , 48, 80
- unary concatenation, 191
- unary representation, 160
- unary search, 166
- unbounded search, 166
- universal
 - strongly \sim coding, 223
 - weakly \sim coding, 223
- universal prior, 242
- universal probability, 10
- value of a game, 237
- variational distance, 56
- weak converse theorem, 87
- weakly consistent estimator, 224
- weight, 146
- window, 202
- Wyner's inequality, 162
- zero-sum game, 237

Selected Titles in This Series

(Continued from the front of this publication)

- 165 **V. V. Ishkhanov, B. B. Lur'e, and D. K. Faddeev**, The embedding problem in Galois theory, 1997
- 164 **E. I. Gordon**, Nonstandard methods in commutative harmonic analysis, 1997
- 163 **A. Ya. Dorogovtsev, D. S. Silvestrov, A. V. Skorokhod, and M. I. Yadrenko**, Probability theory: Collection of problems, 1997
- 162 **M. V. Boldin, G. I. Simonova, and Yu. N. Tyurin**, Sign-based methods in linear statistical models, 1997
- 161 **Michael Blank**, Discreteness and continuity in problems of chaotic dynamics, 1997
- 160 **V. G. Osmolovskii**, Linear and nonlinear perturbations of the operator div, 1997
- 159 **S. Ya. Khavinson**, Best approximation by linear superpositions (approximate nomography), 1997
- 158 **Hideki Omori**, Infinite-dimensional Lie groups, 1997
- 157 **V. B. Kolmanovskii and L. E. Shaikhet**, Control of systems with aftereffect, 1996
- 156 **V. N. Shevchenko**, Qualitative topics in integer linear programming, 1997
- 155 **Yu. Safarov and D. Vassiliev**, The asymptotic distribution of eigenvalues of partial differential operators, 1997
- 154 **V. V. Prasolov and A. B. Sossinsky**, Knots, links, braids and 3-manifolds. An introduction to the new invariants in low-dimensional topology, 1997
- 153 **S. Kh. Aranson, G. R. Belitsky, and E. V. Zhuzhoma**, Introduction to the qualitative theory of dynamical systems on surfaces, 1996
- 152 **R. S. Ismagilov**, Representations of infinite-dimensional groups, 1996
- 151 **S. Yu. Slavyanov**, Asymptotic solutions of the one-dimensional Schrödinger equation, 1996
- 150 **B. Ya. Levin**, Lectures on entire functions, 1996
- 149 **Takashi Sakai**, Riemannian geometry, 1996
- 148 **Vladimir I. Piterbarg**, Asymptotic methods in the theory of Gaussian processes and fields, 1996
- 147 **S. G. Gindikin and L. R. Volevich**, Mixed problem for partial differential equations with quasihomogeneous principal part, 1996
- 146 **L. Ya. Adrianova**, Introduction to linear systems of differential equations, 1995
- 145 **A. N. Andrianov and V. G. Zhuravlev**, Modular forms and Hecke operators, 1995
- 144 **O. V. Troshkin**, Nontraditional methods in mathematical hydrodynamics, 1995
- 143 **V. A. Malyshev and R. A. Minlos**, Linear infinite-particle operators, 1995
- 142 **N. V. Krylov**, Introduction to the theory of diffusion processes, 1995
- 141 **A. A. Davydov**, Qualitative theory of control systems, 1994
- 140 **Aizik I. Volpert, Vitaly A. Volpert, and Vladimir A. Volpert**, Traveling wave solutions of parabolic systems, 1994
- 139 **I. V. Skrypnik**, Methods for analysis of nonlinear elliptic boundary value problems, 1994
- 138 **Yu. P. Razmyslov**, Identities of algebras and their representations, 1994
- 137 **F. I. Karpelevich and A. Ya. Kreinin**, Heavy traffic limits for multiphase queues, 1994
- 136 **Masayoshi Miyanishi**, Algebraic geometry, 1994
- 135 **Masaru Takeuchi**, Modern spherical functions, 1994
- 134 **V. V. Prasolov**, Problems and theorems in linear algebra, 1994
- 133 **P. I. Naumkin and I. A. Shishmarev**, Nonlinear nonlocal equations in the theory of waves, 1994

For a complete list of titles in this series, visit the
AMS Bookstore at www.ams.org/bookstore/.

ISBN 0-8218-4256-0



9 780821 842560

MMONO/203.S

AMS *on the Web*
www.ams.org