

Gareth A. Jones and J. Mary Jones

Information and Coding Theory

With 31 Figures



Springer

Gareth A. Jones, MA, DPhil
Faculty of Mathematical Studies, University of Southampton,
Southampton SO17 1BJ, UK

J. Mary Jones, MA, DPhil
The Open University, Walton Hall, Milton Keynes MK7 6AA, UK

Cover illustration elements reproduced by kind permission of:

Aptech Systems, Inc., Publishers of the GAUSS Mathematical and Statistical System, 23804 S.E. Kent-Kangley Road, Maple Valley, WA 98038, USA. Tel: (206) 432 - 7855 Fax (206) 432 - 7832 email: info@aptech.com URL: www.aptech.com

American Statistical Association: Chance Vol 8 No 1, 1995 article by KS and KW Heiner 'Tree Rings of the Northern Shawangunks' page 32 fig 2

Springer-Verlag: *Mathematica in Education and Research* Vol 4 Issue 3 1995 article by Roman E Maeder, Beatrice Amrhein and Oliver Gloor 'Illustrated Mathematics: Visualization of Mathematical Objects' page 9 fig 11, originally published as a CD ROM 'Illustrated Mathematics' by TELOS: ISBN 978-1-85233-622-6

Mathematica in Education and Research Vol 4 Issue 3 1995 article by Richard J Gaylord and Kazume Nishidate 'Traffic Engineering with Cellular Automata' page 35 fig 2. *Mathematica in Education and Research* Vol 5 Issue 2 1996 article by Michael Trott 'The Implicitization of a Trefoil Knot' page 14.

Mathematica in Education and Research Vol 5 Issue 2 1996 article by Lee de Cola 'Coins, Trees, Bars and Bells: Simulation of the Binomial Process' page 19 fig 3. *Mathematica in Education and Research* Vol 5 Issue 2 1996 article by Richard Gaylord and Kazume Nishidate 'Contagious Spreading' page 33 fig 1. *Mathematica in Education and Research* Vol 5 Issue 2 1996 article by Joe Buhler and Stan Wagon 'Secrets of the Madelung Constant' page 50 fig 1.

ISSN 1615-2085

ISBN 978-1-85233-622-6

British Library Cataloguing in Publication Data

Jones, Gareth A.

Information and coding theory. - (Springer undergraduate mathematics series)

1. Information theory 2. Coding theory

I. Title II. Jones, J. Mary

003.5'4

ISBN 978-1-85233-622-6 ISBN 978-1-4471-0361-5 (eBook)

DOI 10.1007/978-1-4471-0361-5

Library of Congress Cataloging-in-Publication Data

Jones, Gareth A.

Information and coding theory / Gareth A. Jones and J. Mary Jones.

p. cm. -- (Springer undergraduate mathematics series)

Includes bibliographical references and index.

ISBN 978-1-85233-622-6

1. Information theory. 2. Coding theory. I. Jones, J. Mary (Josephine Mary), 1946-

II. Title. III. Series.

Q360 .J68 2000

003'.54—dc21

00-030074

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

© Springer-Verlag London 2000

Originally published by Springer-Verlag London Limited 2000

The use of 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 laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Typesetting: Camera ready by the author and Michael Mackey

12/3830-54321 Printed on acid-free paper SPIN 10866505

Contents

Preface	v
Notes to the Reader	xiii
1. Source Coding	1
1.1 Definitions and Examples	1
1.2 Uniquely Decodable Codes	4
1.3 Instantaneous Codes	9
1.4 Constructing Instantaneous Codes	11
1.5 Kraft's Inequality	13
1.6 McMillan's Inequality	14
1.7 Comments on Kraft's and McMillan's Inequalities	16
1.8 Supplementary Exercises	17
2. Optimal Codes	19
2.1 Optimality	19
2.2 Binary Huffman Codes	22
2.3 Average Word-length of Huffman Codes	26
2.4 Optimality of Binary Huffman Codes	27
2.5 r -ary Huffman Codes	28
2.6 Extensions of Sources	30
2.7 Supplementary Exercises	32
3. Entropy	35
3.1 Information and Entropy	35
3.2 Properties of the Entropy Function	40
3.3 Entropy and Average Word-length	42

3.4	Shannon–Fano Coding	45
3.5	Entropy of Extensions and Products	47
3.6	Shannon’s First Theorem	48
3.7	An Example of Shannon’s First Theorem	49
3.8	Supplementary Exercises	51
4.	Information Channels	55
4.1	Notation and Definitions	55
4.2	The Binary Symmetric Channel	60
4.3	System Entropies	62
4.4	System Entropies for the Binary Symmetric Channel	64
4.5	Extension of Shannon’s First Theorem to Information Channels	67
4.6	Mutual Information	70
4.7	Mutual Information for the Binary Symmetric Channel	72
4.8	Channel Capacity	73
4.9	Supplementary Exercises	76
5.	Using an Unreliable Channel	79
5.1	Decision Rules	79
5.2	An Example of Improved Reliability	82
5.3	Hamming Distance	85
5.4	Statement and Outline Proof of Shannon’s Theorem	88
5.5	The Converse of Shannon’s Theorem	90
5.6	Comments on Shannon’s Theorem	93
5.7	Supplementary Exercises	94
6.	Error-correcting Codes	97
6.1	Introductory Concepts	97
6.2	Examples of Codes	100
6.3	Minimum Distance	104
6.4	Hamming’s Sphere-packing Bound	107
6.5	The Gilbert–Varshamov Bound	111
6.6	Hadamard Matrices and Codes	114
6.7	Supplementary Exercises	118
7.	Linear Codes	121
7.1	Matrix Description of Linear Codes	121
7.2	Equivalence of Linear Codes	127
7.3	Minimum Distance of Linear Codes	131
7.4	The Hamming Codes	133
7.5	The Golay Codes	136
7.6	The Standard Array	141

7.7 Syndrome Decoding	143
7.8 Supplementary Exercises	146
Suggestions for Further Reading	149
Appendix A. Proof of the Sardinas–Patterson Theorem	153
Appendix B. The Law of Large Numbers	157
Appendix C. Proof of Shannon’s Fundamental Theorem	159
Solutions to Exercises	165
Bibliography	191
Index of Symbols and Abbreviations	195
Index	201