

Foundations in Signal Processing, Communications and Networking

Volume 13

Series editors

Wolfgang Utschick, Garching, Germany

Holger Boche, München, Germany

Rudolf Mathar, Aachen, Germany

More information about this series at <http://www.springer.com/series/7603>

Rudolf Ahlswede

Combinatorial Methods and Models

Rudolf Ahlswede's
Lectures on Information Theory 4

Edited by

Alexander Ahlswede

Ingo Althöfer

Christian Deppe

Ulrich Tamm

 Springer

Author

Rudolf Ahlswede (1938–2010)
Department of Mathematics
University of Bielefeld
Bielefeld
Germany

Editors

Alexander Ahlswede
Bielefeld
Germany

Ingo Althöfer
Faculty of Mathematics and Computer
Science
Friedrich-Schiller-University Jena
Jena
Germany

Christian Deppe
Department of Mathematics
University of Bielefeld
Bielefeld
Germany

Ulrich Tamm
Faculty of Business and Health
Bielefeld University of Applied Sciences
Bielefeld
Germany

ISSN 1863-8538

ISSN 1863-8546 (electronic)

Foundations in Signal Processing, Communications and Networking

ISBN 978-3-319-53137-3

ISBN 978-3-319-53139-7 (eBook)

DOI 10.1007/978-3-319-53139-7

Library of Congress Control Number: 2017936898

Mathematics Subject Classification (2010): 94-XX, 94BXX

© Springer International Publishing AG 2018

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, 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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature

The registered company is Springer International Publishing AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

As long as algebra and geometry proceed along separate paths, their advance was slow and their applications limited. But when these sciences joined company, they drew from each other fresh vitality and hence forward marched on at a rapid pace towards perfection.

Joseph Louis Lagrange

Preface¹

After an introduction to classical information theory, we present now primarily own methods and models, which go considerably beyond it. They were also sketched in our Shannon Lecture 2006. There are two main components: our combinatorial approach to information theory in the late 1970s, where probabilistic source and channel models enter via the skeleton, a hypergraph based on typical sequences, and our theory of identification, which is now generalized to a general theory of information transfer (GTIT) incorporating also as ingredient a theory of common randomness, the main issue in cryptology. We begin with methods, at first with collections of basic covering, colouring, and packing lemmas with their proofs, which are based on counting or the probabilistic method of random choice.

Of course, these two methods are also closely related: the counting method can be viewed as the method of random choice for uniform probability distributions. It must be emphasized that there are cases where the probabilistic method fails, but the greedy algorithm (maximal coding) does not or both methods have to be used in combination. A striking example, Gallager's source coding problem, is discussed. Particularly useful is a special case of the Covering Lemma, called the link. It was used by Körner for zero-error problems, which are packing problems, in his solution of Rényi's problem. Very useful are also two methods, the elimination technique and the robustification technique, with applications for AV-theory and unidirectional memories.

Colouring and covering lemmas find also applications in many lectures on combinatorial models of information processing:

- Communication complexity,
- Interactive communication,
- Write-efficient Memories and
- ALOHA.

¹This is the original preface written by Rudolf Ahlswede for the second 1000 pages of his lectures. This volume consists of the first third of these pages.

They are central in the theory of identification, especially in the quantum setting, in the theory of common randomness, and in the analysis of a complexity measure by Ahlswede, Khachatryan, Mauduit, and Sárkozy for number theoretical crypto-systems.

Bielefeld, Germany

Rudolf Ahlswede

Words and Introduction of the Editors

Rudolf Ahlswede was one of the worldwide-accepted experts on information theory. Many key developments in this area are due to him. In particular, he made big progress in multi-user theory. Furthermore, with identification theory, he introduced a new research direction. Rudolf Ahlswede died in December 2010.

The fourth volume of Rudolf Ahlswede's lectures on information theory is focused on combinatorics. Rudolf Ahlswede's original motivation to study combinatorial aspects of information theory problems were zero-error codes: in this case, the structure of the coding problems usually drastically changes from probabilistic to combinatorial. The best example is Shannon's zero-error capacity where independent sets in graphs have to be examined. The extension to multiple access channels leads to the Zarankiewicz problem.

On his initiative, professorships for combinatorics and complexity theory were established in Bielefeld University. He made contacts to the leading institutes worldwide. In his own research, combinatorics became more and more important such that in the big special research unit "Discrete Structures in Mathematics" at Bielefeld University, Rudolf Ahlswede was the head of two projects on "Models with Information Exchange" and "Combinatorics of Sequence Spaces", respectively. Rudolf Ahlswede also became very renowned for his research on combinatorics: let us only mention that with Levon Khachtrian, he settled the famous $4m$ conjecture of Paul Erdős and that the well-known Ahlswede—Daykin inequality (also called Four Function Theorem (FFT)) even takes his name. Bollobas wrote in his book "Combinatorics" about that result:

At the first glance the FFT looks too general to be true and, if true, it seems too vague to be of much use. In fact, exactly the opposite is true: the Four Functions Theorem (FFT) of Ahlswede and Daykin is a theorem from "the book". It is beautifully simple and goes to the heart of the matter. Having proved it, we can sit back and enjoy its power enabling us to deduce a wealth of interesting results. This is precisely the reason why this section is rather long: it would be foolish not to present a good selection of the results one can obtain with minimal effort from the FFT.

The history of the idea of the AD-inequality is very interesting. As Daykin came to a visit to Bielefeld, Ahlswede was just wallpapering. He stood on the ladder, and Daykin wanted to tell him from a newly proven inequality. The declaration was complicated, and Ahlswede said that probably a more general (and easier) theorem should hold. He made directly—on the ladder—a proposal which already was the AD-inequality.

The lecture notes he selected for this volume concentrate on the deep interplay between coding theory and combinatorics. The lectures in Part I (Basic Combinatorial Methods for Information Theory) are based on Rudolf Ahlswede's own research and the methods and techniques he introduced.

A code can combinatorially be regarded as a hypergraph, and many coding theorems can be obtained by appropriate colourings or coverings of the underlying hypergraphs. Several such colouring and covering techniques and their applications are introduced in Chap. 1.

Chapter 2 deals with codes produced by permutations. Finally, in Chap. 3, applications of one of Rudolf Ahlswede's favourite research fields—extremal problems in combinatorics—are presented. In particular, he analysed Kraft's inequality for prefix codes as the LYM property in the poset imposed by a tree. This led to a generalization to arbitrary posets.

Rudolf Ahlswede's results on diametric and intersection theorems were already included in the book *Lectures on Advances in Combinatorics* (with V. Blinovsky).

Whereas the first part concentrates on combinatorial methods in order to analyse classical codes as prefix codes or codes in the Hamming metric, the second part of this book is devoted to combinatorial models in information theory. Here, the code concept already relies on a rather combinatorial structure, as in several concrete models of multiple access channels (Chap. 4) or more refined distortions (Chap. 5). An analytical tool coming into play, especially during the analysis of perfect codes, are orthogonal polynomials (Chap. 6).

Finally, the editors would like to tell a little bit about the state of the art at this point. Rudolf Ahlswede's original plan was to publish his lecture notes containing in total a number of about 4000 pages in three very big volumes. With the publisher, he finally agreed to subdivide each volume in 3–4 smaller books. The first three books which appeared so far, indeed, were the first “big” volume on which Rudolf Ahlswede had concentrated most of his attention, so far, and which was almost completely prepared for publication by himself. Our editorial work with the first three volumes, hence, was mainly to take care of the labels and enumeration of the formulae, theorems, etc., and to correct some minor mistakes. Starting with this volume, the situation is a little different. Because of Rudolf Ahlswede's sudden death, his work here was not yet finished and some chapters were not completed. We decided to delete some sections with which we did not feel comfortable or which were just fragmentary.

Our thanks go to Regine Hollmann, Carsten Petersen, and Christian Wischmann for helping us typing, typesetting, and proofreading. Furthermore, our thanks go to

Bernhard Balkenhol who combined the first approx. 2000 pages of lecture scripts in different styles (AMS-TeX, LaTeX, etc.) to one big lecture script. Bernhard can be seen as one of the pioneers of Ahlswede's lecture notes.

Alexander Ahlswede
Ingo Althöfer
Christian Deppe
Ulrich Tamm

Contents

Part I Combinatorial Methods for Information Theory

1	Covering, Coloring, and Packing Hypergraphs	3
1.1	Covering Hypergraphs	4
1.1.1	Multiple Coverings for Hypergraphs and Approximation of Output Statistics	8
1.2	Coverings, Packings, and Algorithms	9
1.2.1	Fractional Packings and Coverings	9
1.2.2	A Greedy Algorithm to Estimate $\tau(\mathcal{H})$, $\tau^*(\mathcal{H})$ from Above	11
1.2.3	Applications	13
1.3	Application to the k -Tuple Chromatic Number χ_k	14
1.4	On a Problem of Shannon in Graph Theory	14
1.4.1	Introduction	14
1.5	A Necessary and Sufficient Condition in Terms of Linear Programming for G to be Universal	15
1.5.1	Shannon's Condition Is Not Necessary	16
1.5.2	Characterizing Universality in Terms of Integer Linear Programming	18
1.6	The Basic Coloring Lemmas	19
1.6.1	Colorings Which Are Good in All Edges	19
1.7	Colorings Which Are Good in Average	25
1.7.1	Weighted Hypergraphs	25
1.7.2	Orthogonal Colorings	27
1.7.3	Universal Colorings of Internally Weighted Hypergraphs	28
1.8	Orthogonal Coloring of Rectangular Hypergraphs $(\mathcal{V} \times \mathcal{W}, \mathcal{E})$	31
1.8.1	Types of Edges and Partitioning into Diagonals	32
1.8.2	Coloring Most Points Correctly in Their Neighborhood	34

- 1.8.3 One-Sided Balanced Colorings of Rectangular Hypergraphs 35
- 1.8.4 Orthogonal Coloring of a Long Diagonal Within an Edge 36
- 1.9 Balanced Colorings 38
- 1.10 Color Carrying Lemma and Other Concepts and Results 43
 - 1.10.1 Color Carrying Lemma 43
 - 1.10.2 Other Basic Concepts 44
- References 46
- Further Readings 46
- 2 Codes Produced by Permutations: The Link Between Source and Channel Coding 57**
 - 2.1 Introduction 57
 - 2.2 Notation and Known Facts 59
 - 2.3 The Main Result: Channel Codes Produced by Permutations 63
 - 2.4 Correlated Source Codes Produced by Permutations from Ordinary Channel Codes 69
 - 2.5 An Iterative Code Construction Achieving the Random Coding and the Expurgated Bound 74
 - 2.6 Good Codes Are Highly Probable 80
 - References 87
 - Further Readings 88
- 3 Results for Classical Extremal Problems 89**
 - 3.1 Antichains 89
 - 3.1.1 Kraft’s Inequality and the LYM-property 89
 - 3.1.2 Ahlswede–Zhang Identity 93
 - 3.1.3 Sperner’s Lemma and Its Original Proof 95
 - 3.2 On Independence Numbers in Graphs 98
 - 3.3 A Combinatorial Partition Problem: Baranyai’s Theorem 99
 - 3.4 More on Packing: Bounds on Codes 105
 - 3.4.1 Plotkin’s Bound 105
 - 3.4.2 Johnson’s Bounds 106
 - 3.4.3 Basic Methods of Proving Gilbert-Type Bounds on the Cardinality of a Code 107
 - References 109
- Part II Combinatorial Models in Information Theory**
- 4 Coding for the Multiple-Access Channel: The Combinatorial Model 113**
 - 4.1 Coding for Multiple-Access Channels 113
 - 4.1.1 Basic Definitions 113
 - 4.1.2 Achievable Rate Region Under the Criterion of Arbitrarily Small Average Decoding Error Probability 116

- 4.2 Coding for the Binary Adder Channel. 121
 - 4.2.1 Statement of the Problem of Constructing UD Codes 121
 - 4.2.2 Rates of UD Codes $(\mathcal{U}, \mathcal{V})$ when \mathcal{U} and \mathcal{V} are Linear Codes. 122
 - 4.2.3 Rates of UD Codes $(\mathcal{U}, \mathcal{V})$ when \mathcal{U} is a Linear Code 124
 - 4.2.4 Constructing UD Codes 134
 - 4.2.4.1 Code Construction (u)–(v) 136
 - 4.2.4.2 Properties of Codes Constructed by (u)–(v) . . . 138
 - 4.2.4.3 Decoding Algorithm 142
 - 4.2.4.4 Enumerative Coding 143
 - 4.2.5 Coding for the T-User Binary Adder Channel 146
- 4.3 On the T-User q-Frequency Noiseless Multiple-Access Channel without Intensity Information 155
 - 4.3.1 Introduction 156
 - 4.3.2 Information-Theoretic Bounds 157
 - 4.3.3 Construction of Codes for the A Channel 160
 - 4.3.3.1 Construction (A-1) 161
 - 4.3.3.2 Construction (A-2) 162
 - 4.3.3.3 Construction (A-3) 162
 - 4.3.4 Evaluation of the Asymptotics of the Summarized Capacity of a T-User q-Frequency Noiseless Multiple-Access Channel 163
- 4.4 Nearly Optimal Multi-user Codes for the Binary Adder Channel. 170
 - 4.4.1 Introduction 170
 - 4.4.2 Two Multi-user Codes 172
 - 4.4.2.1 Preliminaries 172
 - 4.4.2.2 Construction A 174
 - 4.4.2.3 Construction B 179
 - 4.4.3 Performance 181
 - 4.4.3.1 Capacity and Majorization 181
 - 4.4.3.2 Codes Constructed from \mathcal{U}_A^j 182
 - 4.4.3.3 Codes Constructed from \mathcal{U}_B^j 186
 - 4.4.4 The T-User, q-Frequency Adder Channel 187
 - 4.4.5 Concluding Remarks 192
- 4.5 Coding for the Binary Switching Channel 194
 - 4.5.1 UD Codes for the Binary Switching Channel 194
 - 4.5.1.1 Proof of Theorem 4.24 197
- 4.6 Coding for Interference Channels 198
 - 4.6.1 Statement of the Coding Problem for Interference Channels. 198
 - 4.6.2 The Sandglass Conjecture 200

- 4.7 UD Codes for Multiple-Access Adder Channels Generated by Integer Sets. 204
 - 4.7.1 Statement of the Problem 204
 - 4.7.2 Code Design 207
 - 4.7.3 UD Codes in $\{0, 1\}^n$ 208
- 4.8 Coding for the Multiple-Access Channels with Noiseless Feedback 209
 - 4.8.1 Example of an Information Transmission Scheme over the Binary Adder Channel 209
 - 4.8.2 Cover–Leung Coding Scheme 210
- 4.9 Some Families of Zero-Error Block Codes for the Two-User Binary Adder Channel with Feedback. 214
 - 4.9.1 Introduction 214
 - 4.9.2 Two Families of Codes for the Binary Adder Channel with Partial Feedback 215
 - 4.9.2.1 The First Family of Codes 216
 - 4.9.2.2 Rate Pairs and Rate Sum 217
 - 4.9.2.3 The Second Family of Codes 217
 - 4.9.3 Codes Generated by Difference Equations. 219
 - 4.9.3.1 Square Dividing Strategy 219
 - 4.9.3.2 Fibonacci Codes 221
 - 4.9.3.3 The Inner Bound to the Zero-Error Capacity Region 224
 - 4.9.4 Codes Generated by Difference Equations for the Binary Adder Channel with Full Feedback 225
 - 4.9.4.1 Refinement of the Fibonacci Code 225
 - 4.9.4.2 Inner Bound for the Zero-Error Capacity Region of a Binary Adder Channel with Full Feedback 225
 - 4.9.5 Proof of Theorem 4.29 via Three Lemmas 226
- References 228
- Further Readings 230
- 5 Packing: Combinatorial Models for Various Types of Errors 233**
 - 5.1 A Class of Systematic Codes. 233
 - 5.1.1 Basic Definitions 233
 - 5.1.2 Construction of a Maximal d-Code. 234
 - 5.1.3 Estimation of the Size 236
 - 5.1.4 The Practical Construction 238
 - 5.2 Asymptotically Optimum Binary Code with Correction for Losses of One or Two Adjacent Bits. 239
 - 5.2.1 Codes with Correction for Losses of 1 or Fewer Adjacent Bits 239
 - 5.2.2 Upper Estimate of the Size of Binary Codes with Correction for Losses of 1 Adjacent Bits 240

5.2.3	A Class of Binary Codes with Correction for Losses of One or Two Adjacent Bits	241
5.2.4	Size of Codes B_n^q	245
5.3	Single Error-Correcting Close-Packed and Perfect Codes	246
5.3.1	Introduction	247
5.3.2	The Criterion of Unique Decodability (UD)	249
5.3.3	$\{1, -1\}$ -Type Error-Correcting Codes	249
5.3.4	$\{1, 2\}$ - or $\{-1, -2\}$ -Type Error-Correcting Codes	251
5.3.5	$\{+1, -1, +2, -2\}$ -Type Error-Correcting Codes	257
5.3.6	A Formula for Computing Powers of Codes Defined by Congruences	263
5.4	Constructing Defect-Correcting Codes	272
5.5	Results for the Z-Channel	277
5.5.1	Introduction	277
5.5.2	Upper Bounds	277
5.5.3	Single Error-Correcting Codes	280
5.5.4	Error Burst Correction	282
5.6	On q -Ary Codes Correcting All Unidirectional Errors of a Limited Magnitude	283
5.6.1	Introduction	283
5.6.2	Distances and Error-Correcting Capabilities	286
5.6.3	ℓ -AEC Codes	287
5.6.4	ℓ -UEC Codes	288
5.6.5	ℓ -UEC Codes of Varshamov–Tennengol’s Type	291
5.6.6	Lower and Upper Bounds for $LA_u(n, \ell)_q$	293
5.6.7	Construction of Optimal Codes	295
5.6.8	Asymptotic Growth Rate of ℓ -UEC Codes of VT Type	299
5.6.9	The Error Detection Problem	301
	References	302
	Further Readings	304
6	Orthogonal Polynomials in Information Theory	307
6.1	Introduction	307
6.1.1	Orthogonal Polynomials	307
6.2	Splittings of Cyclic Groups and Perfect Shift Codes	310
6.2.1	Introduction	310
6.2.2	Factorizations of \mathbb{Z}_p^* and $\mathbb{Z}_p^*/\{1, -1\}$ with the Set $\{1, a, \dots, a^r, b, \dots, b^s\}$	314
6.2.3	Computational Results on Splittings and Perfect 3- and 4-Shift Codes	319
6.2.4	Tilings by the Cross and Semicross and Splittings of Groups of Composite Order	322
6.2.5	Concluding Remarks	324
6.3	Some Aspects of Hankel Matrices in Coding Theory and Combinatorics	326

- 6.3.1 Introduction 326
- 6.3.2 Hankel Matrices and Chebyshev Polynomials 332
- 6.3.3 Generalized Catalan Numbers and Hankel
Determinants 337
- 6.3.4 Alternating Sign Matrices 343
- 6.3.5 Catalan-Like Numbers and the Berlekamp-Massey
Algorithm 346
- 6.3.6 Lattice Paths not Touching a Given Boundary 353
- References 368
- Further Readings 373
- Appendix A: Supplement 375**
- Author Index 379**
- Subject Index 383**