Foundations in Signal Processing, Communications and Networking

Volume 13

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

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 Langrange

Preface[1]

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.

[1]This 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, Khachatrian, 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 Erdös 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 Ahlswedes' 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