Foundations in Signal Processing, Communications and Networking

Volume 16

Series Editors
Holger Boche, Technische Universität München, München, Germany
Rudolf Mathar, RWTH Aachen University, ICT cubes, Aachen, Germany
Wolfgang Utschick, Technische Universität München, München, Germany

This book series presents monographs about fundamental topics and trends in signal processing, communications and networking in the field of information technology. The main focus of the series is to contribute on mathematical foundations and methodologies for the understanding, modeling and optimization of technical systems driven by information technology. Besides classical topics of signal processing, communications and networking the scope of this series includes many topics which are comparably related to information technology, network theory, and control. All monographs will share a rigorous mathematical approach to the addressed topics and an information technology related context.

** Indexing: The books of this series are indexed in Scopus and zbMATH **

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

Rudolf Ahlswede

Identification and Other Probabilistic Models

Rudolf Ahlswede's Lectures on Information Theory 6

Alexander Ahlswede • Ingo Althöfer • Christian Deppe • Ulrich Tamm
Editors

Springer

Author
Rudolf Ahlswede (deceased)
Bielefeld, Germany

Editors
Alexander Ahlswede
Bielefeld, Germany

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

Christian Deppe
Institute for Communications Engineering
Technical University of Munich
München, Germany

Ulrich Tamm
Fachbereich Wirtschaft und Gesundheit
Fachhochschule Bielefeld
Bielefeld, Germany

ISSN 1863-8538 ISSN 1863-8546 (electronic)
Foundations in Signal Processing, Communications and Networking
ISBN 978-3-030-65070-4 ISBN 978-3-030-65072-8 (eBook)
https://doi.org/10.1007/978-3-030-65072-8

© Springer Nature Switzerland AG 2021, corrected publication 2021
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, expressed 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.

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Words and Introduction of the Editors

Rudolf Ahlswede was one of the worldwide accepted experts on information theory. Many main developments in this area are due to him. Especially, he made big progress in multi-user theory. Furthermore, with identification theory and network coding, he introduced new research directions. Ahlswede died in December 2010.

Several highlights of Ahlswede's research are the Ahlswede-Daykin inequality and the Ahlswede-Khachatrian complete intersection theorem, which even include his name. He also described the capacity region of the multiple-access channel (many senders, one receiver). Together with Tom Cover's corresponding result for the broadcast channel (one sender, several receivers), this is the theoretical backbone for many algorithms in mobile communication, for instance, in the 5G standard. In 1990 jointly with his student Gunter Dueck, he initiated a whole new area of research—the theory of identification. Gunter Dueck in the supplement of this volume describes how things got started in this direction. Their paper found immediate interest. Shortly after its appearance, Ahlswede and Dueck received the Best Paper Award of the IEEE Information Theory Society. This is very much remarkable, especially, when taking into account that Ahlswede had received this award only two years before for his joint work with Imre Csiszar—it is quite extraordinary that the same author is honored with such an important award twice in such a short time.

This whole volume is devoted to identification and related concepts. In classical information theory, a sender transmits a message to a receiver over a noisy channel. The question that has to be answered at the receiving end hence is "Which message was sent?". Claude Shannon derived the famous channel capacity C: approximately 2^{nC} messages can be sent over the channel, such that the receiver can still reliably answer this question, where the message length n tends to infinity. Ahlswede and Dueck considered a new scenario, in which the receiver now has to answer the question: "Is this the message the one I am interested in?" This might be illustrated with the following example where a car owner (the sender) presses the button of his key and his car (the receiver) opens the door automatically. To obtain this result, a code is transmitted and the receiver is not really interested in the question which car should be opened but only if the car itself should be opened or not. In order to reliably answer this question, two conditions have to be guaranteed: (1) The car of interest should open (with very high probability) and (2) no other car should open its door when receiving the transmitted signal. Ahlswede and Dueck found that also for this problem a capacity theorem exists. Approximately, $2^{2^{nC}}$ messages can be identified over the same noisy channel. Surprisingly, the number C, i.e., the identification capacity, is the same as Shannon's capacity for transmission. However, now, the expression is doubly exponential.

In the sequel, Ahlswede was working intensively on a general theory of information transfer that should include transmission and identification of information as special cases. To this aim, he was awarded a prestigious project in the center for interdisciplinary research (ZiF) in Bielefeld. Actually, this work occupied him for the rest of his life and was also the main reason for the delay of these lecture notes. He wanted to publish them when the general theory of information transfer was mature to some degree. For instance, his research led to the conjecture that the non-secure identification capacity (C_{ID}) might be the same as the common randomness capacity (C_{CR}) for channels without extra resources (like feedback). His student Christian Kleinewächter found a counterexample in which $C_{\mathrm{CR}} > C_{\mathrm{ID}}$. Ahlswede himself also showed that $C_{\mathrm{ID}} > C_{\mathrm{CR}}$ can hold (see 6). In his Shannon Lecture 2006 at the IEEE Symposium on Information Theory in Seattle, Ahlswede mentioned that this conjecture had helped him in the derivation of further capacity results.

As this example shows, the analysis of information identification led to many new concepts and problems. Source coding and data compression for identification are different from the corresponding concepts in information transmission. New probabilistic algorithms and the underlying randomness had to be studied. Further, there is a strong relation to hypothesis testing, when hypotheses have to be discriminated. All these directions are presented and studied in the corresponding chapters of this volume.

Chapter "Testing of Hypotheses and Identification" are lecture notes that were prepared by Marat Burnashev for a lecture he gave in Bielefeld in 2001. Ahlswede later used his notes for his lecture. We thank Marat Burnashev for allowing us to add his text in this book. Furthermore, we add Part VI to the book, which is a survey by Holger Boche, Christian Deppe, and Wafa Labidi of results in the theory of identification in the last 10 years.

Special thanks go to Wafa Labidi for the sixth volume. She has put a lot of work into creating index directories, proofreading, and rewriting. We also thank Gerhard Kramer for his support by financing Wafa Labidi. Finally, our thanks go to Bernhard Balkenhol who combines the first approximately 2000 pages of lecture scripts in different styles (AMS-TeX, LaTeX, etc.) to one big lecture script. He can be seen as one of the pioneers of Ahlswede's lecture notes.

Alexander Ahlswede, Ingo Althöfer, Christian Deppe, Ulrich Tamm

Preface

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 seventies, 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, coloring, and packing lemmata 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 arbitrarily varying channel and unidirectional memories.

Coloring and covering lemmata find also applications in many lectures on combinatorial models of information processing: communication complexity, interactive communication, write-efficient memories, ALOHA. 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[1]

[1]This is the original preface written by Rudolf Ahlswede for the second 1.000 pages of his lectures. This volume consists of the last third of these pages.

Preamble

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

Contents

Notation and Abbreviations

$< x^n \| x >$	Number of occurrences of letter x in sequence x^n
$\| \cdot \|_1$	Statistical distance
1_A	Characteristic function of set A
A^c	Complement of set A
A-code	Average-list-size code
AVC	Arbitrarily-varying channel
AVWC	Arbitrarily-varying wiretap channel
C	Channel capacity
CC	Compound channel
CR	Common randomness
CWC	Compound Wiretap Channel
$D(X\|\|Y)$	I-divergence between X and Y
$D(X\|\|Y\|P)$	Conditional I-divergence between X and Y given P
DMC	Discrete memoryless channel
ED	Empirical distribution
$\mathbb{E}(X)$	Expectation of X
$H(X)$	Entropy of X
$H(X\|Y)$	Conditional entropy of X given Y
ID	Identification
IDF	Identification with feedback
IDf	Identification with passive feedback
$I(X \wedge Y)$	Mutual information between X and Y
$I(P, W)$	Mutual information between P and PW
$M(n, \lambda)$	Max. codesize for transmission codes
$\mu(A)$	Lebesgue measure of set A
NRA	Non-randomized (deterministic) average-list-size
NRI	Non-randomized (deterministic) identification
NRS	Non-randomized (deterministic) separation
$\mathbb{N}$	Natural numbers
$N(n, \lambda)$	Max. codesize for ID codes
PD	Probability distribution

$\mathcal{P}(A)$	The set of all probability distributions on the set A
$\mathbb{R}$, $\mathbb{R}^+$	Real and positive real numbers
RV	Random variable
SAVC	Strongly-arbitrarily-varying channel
SP	Separation
UCR	Uniform Common Randomness
V, W	Stochastic matrices
$W(\cdot\|i)$	$i - th$ row of W
WIDSI	Watermarking IDentification with side information at transmitter and receiver
WIDK	Watermarking IDentification with secure key
wtf	wiretap with feedback