

# **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,  $2^{2^{n^C}}$  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 Klenewächter found a counterexample in which  $C_{CR} > C_{ID}$ . Ahlswede himself also showed that  $C_{ID} > C_{CR}$  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<sup>1</sup>

---

<sup>1</sup>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

## Part I Identification via Channels

<b>Identification via Channels</b> .....	3
1 Results and Preliminaries.....	4
1.1 Notation and Known Facts.....	4
1.2 Formulation of the Identification Problem.....	8
2 The Direct Parts of the Coding Theorems.....	14
3 The Strong Converses.....	23
3.1 Analytic Proof of the Strong Converse.....	23
3.2 Combinatorial Proof of the Strong Converse.....	37
4 Discussion.....	41
References.....	42

## Identification in the Presence of Feedback: A Discovery of New

<b>Capacity Formulas</b> .....	45
1 The Results.....	46
2 Notation and Known Facts.....	49
3 New Proof of the Direct Part in Theorem 12.....	50
4 Proof of the Direct Part of Theorem 40.....	54
5 Proof of the Direct Part of Theorem 41.....	57
6 Proof of the Converse Part of Theorem 40.....	57
7 Proof of the Converse Part of Theorem 41.....	60
References.....	61

## On Identification via Multi-Way Channels with Feedback:

<b>Mystery Numbers</b> .....	63
1 Introduction.....	63
2 Review of Known Concepts and Results.....	64
3 A General Model for Communication Systems.....	67
4 Classes of Feedback Strategies, Common Random Experiments and Their Mystery Numbers.....	68
5 Main Theorem and Consequences.....	70

6	A Method for Proving Converses in Case of Feedback .....	74
7	A 3-Step ID Scheme for the Noiseless BSC .....	76
8	Extension of the 3-Step ID Scheme to the DMC With and Without Feedback .....	77
9	Proof of Theorems 53 and 54 .....	78
10	Proof of Theorem 61, Optimality of Our Coding Scheme .....	80
	References .....	82
	<b>Identification Without Randomization</b> .....	83
1	Introduction and Results .....	84
2	Proof of Theorem 67 .....	90
3	Proof of Theorem 69 .....	93
4	Proof of Theorem 70 .....	94
5	Proof of Theorem 71 .....	95
6	Proof of Lemma 73 .....	97
7	Proof of Theorem 74 .....	99
	References .....	101
	<b>Identification via Channels with Noisy Feedback</b> .....	103
1	Introduction .....	103
2	Proof of Theorem 75 .....	106
	References .....	115
	<b>Identification via Discrete Memoryless Wiretap Channels</b> .....	117
1	Introduction .....	117
2	Proof of Theorem 87 .....	120
	References .....	130
	<b>Part II A General Theory of Information Transfer</b>	
	<b>Introduction</b> .....	133
	References .....	136
	<b>One Sender Answering Several Questions of Receivers</b> .....	137
1	A General Communication Model for One Sender .....	137
2	Analysis of a Specific Model: $\mathbf{K}$ -Identification .....	142
3	Models with Capacity Equal to the Ordinary Capacity .....	153
	References .....	155
	<b>Models with Prior Knowledge of the Receiver</b> .....	157
1	Zero-error Decodable Hypergraphs .....	157
2	$\mathbf{K}$ -Separating Codes .....	158
3	Analysis of a Model with Specific Constraints: 2-Separation and Rényi's Entropy $\mathbf{H}_2$ .....	161
4	Binning via Channels .....	162
5	$\mathbf{K}$ -Identifiability, $\mathbf{K}$ -Separability and Related Notions .....	163
	References .....	165

<b>Models with Prior Knowledge at the Sender</b> .....	167
1 Identification via Group Testing and a Stronger Form of the Rate-Distortion Theorem .....	167
References .....	169
<b>Identification and Transmission with Multi-way Channels</b> .....	171
1 Simultaneous Transfer: Transmission and Identification .....	171
2 A Proof of the Weak Converse to the Identification Coding Theorem for the DMC .....	174
3 Two Promised Results: Characterisation of the Capacity Regions for the MAC and the BC for Identification .....	181
4 The Proof for the MAC .....	184
5 The Proof for the BC .....	188
References .....	190
<b>Data Compression</b> .....	191
1 Noiseless Coding for Identification .....	191
2 Noiseless Coding for Multiple Purposes .....	193
References .....	197
<b>Perspectives</b> .....	199
1 Comparison of Identification Rate and Common Randomness Capacity: Identification Rate can Exceed Common Randomness Capacity and Vice Versa .....	199
2 Robustness, Common Randomness and Identification .....	201
3 Beyond Information Theory: Identification as a New Concept of Solution for Probabilistic Algorithms .....	202
References .....	202
<b>Part III Identification, Mystery Numbers, or Common Randomness</b>	
<b>The Role of Common Randomness in Information Theory and Cryptography: Secrecy Constraints</b> .....	207
1 Introduction .....	207
2 Generating a Shared Secret Key When the Third Party Has No Side Information .....	209
3 Secret Sharing When the Third Party Has Side Information .....	216
4 Proofs .....	220
5 Conclusions .....	227
References .....	228
<b>Common Randomness in Information Theory and Cryptography</b>	
<b>CR Capacity</b> .....	231
1 Introduction .....	231
2 Preliminaries .....	235
2.1 Model (i): Two-Source with One-Way Communication .....	235

2.2	Model (ii): DMC with Active Feedback .....	237
2.3	Model (iii): Two-Source with Two-Way Noiseless Communication .....	239
2.4	Models with Robust CR.....	239
3	Some General Results .....	242
4	Common Randomness in Models (i), (ii), and (iii).....	249
5	Common Randomness, Identification, and Transmission for Arbitrarily Varying Channels.....	262
5.1	Model (A): AVC Without Feedback and Any Other Side Information .....	262
5.2	Model (B): AVC with Noiseless (Passive) Feedback .....	264
5.3	Model (C): Strongly Arbitrarily Varying Channel (SAVC) .....	266
	References .....	268

### **Watermarking Identification Codes with Related Topics on**

	<b>Common Randomness</b> .....	271
1	Introduction .....	272
2	The Notation .....	275
3	The Models.....	275
3.1	Watermarking Identification Codes .....	275
3.2	The Common Randomness .....	279
3.3	The Models for Compound Channels .....	282
4	The Results.....	284
4.1	The Results on Common Randomness .....	284
4.2	The Results on Watermarking Identification Codes .....	286
4.3	A Result on Watermarking Transmission Code with a Common Experiment Introduced by Steinberg-Merhav .....	287
5	The Direct Theorems for Common Randomness.....	288
6	The Converse Theorems for Common Randomness .....	310
7	Construction of Watermarking Identification Codes from Common Randomness .....	317
8	A Converse Theorem of a Watermarking Coding Theorem Due to Steinberg-Merhav .....	318
	References .....	324

### **Transmission, Identification and Common Randomness Capacities for Wire-Tap Channels with Secure Feedback from the Decoder** .....

		327
1	Introduction .....	327
2	Notation and Definitions.....	328
3	Previous and Auxiliary Results .....	329
4	The Coding Theorem for Transmission and Its Proof.....	331
5	Capacity of Two Special Families of Wire-Tap Channels .....	337
6	Discussion: Transmission, Building Common Randomness and Identification.....	340

7	The Secure Common Randomness Capacity in the Presence of Secure Feedback .....	343
8	The Secure Identification Capacity in the Presence of Secure Feedback .....	345
	References .....	347

### **Secrecy Systems for Identification Via Channels with Additive-Like Instantaneous Block Encipherer .....**

1	Introduction .....	349
2	Background .....	350
3	Model .....	352
4	Main Result .....	354
	References .....	357

## **Part IV Identification for Sources, Identification Entropy, and Hypothesis Testing**

<b>Identification for Sources</b> .....		361
1	Introduction .....	361
1.1	Pioneering Model .....	361
2	A Probabilistic Tool for Generalized Identification .....	364
3	The Uniform Distribution .....	367
4	Bounds on $\mathbf{L}(\mathbf{P})$ for General $\mathbf{P} = (\mathbf{P}_1, \dots, \mathbf{P}_N)$ .....	368
4.1	An Upper Bound .....	368
5	An Average Identification Length.....	369
5.1	$\mathbf{Q}$ is the Uniform Distribution on $\mathcal{V} = \mathcal{U}$ .....	370
5.2	The Example Above in Model GID with Average Identification Length for a Uniform $\mathbf{Q}^*$ .....	371
References .....		373

<b>Identification Entropy</b> .....		<b>375</b>
1	Introduction .....	376
2	Noiseless Identification for Sources and Basic Concept of Performance .....	378
3	Examples for Huffman Codes .....	379
4	An Identification Code Universally Good for all <b>P</b> on $\mathcal{U} = \{\mathbf{1}, \mathbf{2}, \dots, \mathbf{N}\}$ .....	383
5	Identification Entropy $\mathbf{H_I(P)}$ and Its Role as Lower Bound .....	384
6	On Properties of $\bar{\mathbf{L}}(\mathbf{P^N})$ .....	387
	6.1 A First Idea .....	389
	6.2 A Rearrangement .....	390
7	Upper Bounds on $\bar{\mathbf{L}}(\mathbf{P^N})$ .....	391
8	The Skeleton .....	393
9	Directions for Research .....	395
References .....		396

<b>An Interpretation of Identification Entropy</b> .....	399
1 Introduction .....	399
1.1 Terminology .....	399
1.2 A New Terminology Involving Proper Common Prefices .....	401
1.3 Matrix Notation .....	402
2 An Operational Justification of ID-Entropy as Lower Bound for $L_C(\mathbf{P}, \mathbf{P})$ .....	405
3 An Alternative Proof of the ID-Entropy Lower Bound for $L_C(\mathbf{P}, \mathbf{P})$ ....	406
4 Sufficient and Necessary Conditions for a Prefix Code $\mathcal{C}$ to Achieve the ID-Entropy Lower Bound of $L_C(\mathbf{P}, \mathbf{P})$ .....	412
5 A Global Balance Principle to Find Good Codes .....	417
6 Comments on Generalized Entropies .....	423
References .....	427
<b>L-Identification for Sources</b> .....	429
1 Introduction .....	429
2 Definitions and Notation .....	434
2.1 Source Coding and Code Trees .....	436
2.2 L-Identification .....	438
3 Two New Results for (1-)Identification .....	440
3.1 (1-)Identification for Block Codes .....	441
3.2 An Improved Upper Bound for Binary Codes .....	444
4 L-Identification for the Uniform Distribution .....	448
4.1 Colexicographic Balanced Huffman Trees .....	450
4.2 An Asymptotic Theorem .....	452
5 Two-Identification for General Distributions .....	461
5.1 An Asymptotic Approach .....	463
5.2 The $q$ -ary Identification Entropy of Second Degree .....	478
5.3 An Upper Bound for Binary Codes .....	487
6 L-Identification for General Distributions .....	490
7 L-Identification for Sets .....	498
8 Open Problems .....	503
8.1 Induction Base for the Proof of Proposition 243 .....	503
8.2 L-Identification for Block Codes .....	506
8.3 L-Identification for Sets for General Distributions .....	508
References .....	510
<b>Testing of Hypotheses and Identification</b> .....	513
1 Preliminaries: Testing of Hypotheses and $L_1$ -Distance .....	513
2 Measures Separated in $L_1$ -Metrics .....	520
3 Identification Codes or “How Large is the Set of all Output Measures for Noisy Channel?” .....	527
References .....	542

**On Logarithmically Asymptotically Optimal Testing of**

<b>Hypotheses and Identification</b> .....	543
1 Problem Statement .....	543
2 Background .....	546
3 Identification Problem for Model with Independent Objects .....	550
4 Identification Problem for Models with Different Objects .....	553
5 Identification of the Probability Distribution of an Object .....	553
6 $r$ -Identification and Ranking Problems .....	557
7 Conclusion and Extensions of Problems .....	563
References .....	564

**On Error Exponents in Quantum Hypothesis Testing** ..... 567

1 Introduction .....	567
2 Definition and Main Results .....	568
3 Bounds on Error Probabilities .....	571
4 Proof of Theorem 278 and the Quantum Stein's Lemma .....	573
5 Toward Further Investigations .....	575
6 Concluding Remarks .....	578
7 Definition of Pinching .....	578
8 Key Operator Inequality .....	579
References .....	580

**Part V Identification and Statistics**

<b>Identification via Compressed Data</b> .....	583
1 Introduction and Formulation of the Problem .....	583
2 Statement and Discussion of the Main Results .....	588
3 Inherently Typical Subset Lemma .....	599
4 Proofs of Theorems 288 and 290 .....	607
5 Proofs of Theorems 5 and 6 .....	628
6 Open Problems .....	635
References .....	635

**Part VI Recent Results**

<b>New Results in Identification Theory</b> .....	639
1 Secure and Robust Identification Against Eavesdropping and Jamming Attacks .....	641
1.1 Compound Channels .....	641
1.2 Arbitrarily-Varying Channels .....	642
1.3 Compound Wiretap Channels .....	643
1.4 Arbitrarily-Varying Wiretap Channels .....	644
2 Classical-Quantum Channels .....	645
2.1 Classical-Quantum Channels .....	645
2.2 Wiretap Classical-Quantum Channels .....	646
2.3 Compound Classical-Quantum Channels .....	647

2.4	Compound Wiretap Classical-Quantum Channels .....	649
2.5	Arbitrarily-Varying Classical-Quantum Channels .....	650
2.6	Arbitrarily-Varying Wiretap Classical-Quantum Channels .....	652
3	Quantum Channels .....	654
4	Classical Gaussian Channels .....	657
4.1	Classical Gaussian Wiretap Channels .....	658
5	Identification and Continuity .....	661
5.1	Basic Definitions and Results .....	661
5.2	Continuity and Discontinuity Behavior of $C_{ID}$ .....	663
5.3	Additivity and Super-Additivity of $C_{ID}$ .....	664
5.4	Continuity of $C_{SID}$ for AVWCs .....	665
5.5	Super-Additivity and Super-Activation for $C_{SID}$ .....	667
6	Identification and Computability .....	668
7	Converse Coding Theorems for Identification via Channels .....	671
7.1	Main Results .....	671
7.2	Average Error Criterion .....	672
8	Converse Coding Theorems for Identification via Multiple Access Channels .....	674
8.1	Identification via Multiple Access Channels .....	674
8.2	Main Results .....	676
9	Explicit Constructions for Identification .....	678
9.1	Conditions for Achieving Identification Capacity .....	680
9.2	A Simple Achievability Proof of Identification .....	683
10	Secure Storage for Identification .....	684
10.1	Storage for Identification Model .....	685
10.2	Results on Common Randomness and Secret Key Generation ....	687
10.3	Achievability Result for Secure Storage for Identification .....	689
10.4	Storage for Identification Model with Two Sources .....	689
10.5	Achievability Definition Two Sources .....	690
11	Secure Communication and Identification Systems: Effective Performance Evaluation on Turing Machines .....	691
11.1	Verification Framework .....	692
11.2	Communication Scenarios .....	694
11.3	Computability of Communication Scenarios .....	695
11.4	General Computability Analysis .....	696
11.5	Channel with an Active Jammer .....	697
11.6	Wiretap Channel with an Active Jammer .....	698
11.7	Computability of Identification Scenarios .....	698
12	Code Reverse Engineering Problem for Identification Codes .....	700
12.1	CRE for Identification Codes .....	700
12.2	Application to BCCK Protocol .....	701
13	Discrete Identification .....	703
14	Private Interrogation of Devices via Identification Codes .....	704
14.1	Identification Codes .....	704
14.2	Protocol for Interrogation .....	705



14.3 Security Analysis .....	706
15 Applications of Identification .....	707
16 Omnisophie .....	709
References .....	710
<b>Correction to: Identification and Other Probabilistic Models .....</b>	<b>C1</b>
<b>Supplement .....</b>	<b>715</b>
1 Abschied—Ein Gedicht von Alexander Ahlswede .....	715
2 Gunter Dueck: Memories of Rudolf Ahlswede.....	716
<b>Author Index .....</b>	<b>721</b>
<b>Subject Index .....</b>	<b>723</b>

# Notation and Abbreviations

$\langle x^n   x \rangle$	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