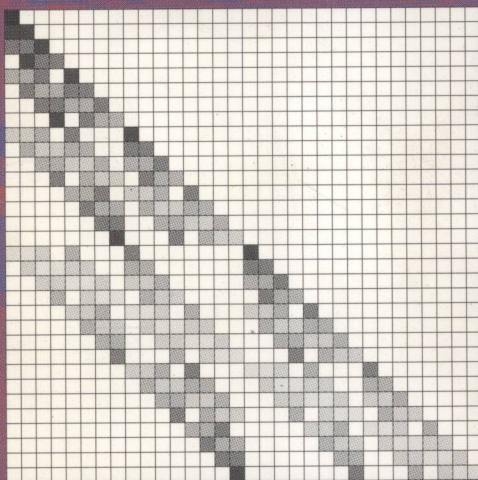


State-of-the-Art
Survey

LNCS 4123

Rudolf Ahlswede et al. (Eds.)

General Theory of Information Transfer and Combinatorics



TN/911-
G 326

Rudolf Ahlswede

Lars Bäumer Ning Cai

Harout Aydinian Vladimir Blinovsky

Christian Deppe Haik Mashurian (Eds.)

General Theory of Information Transfer and Combinatorics



Springer



E2007001418

Volume Editors

Edited by:

Rudolf Ahlswede

Universität Bielefeld, Fakultät für Mathematik

Universitätsstr. 25, 33615 Bielefeld, Germany

E-mail: ahlswede@math.uni-bielefeld.de

Assisted by:

Lars Bäumer

Ning Cai

Universität Bielefeld, Fakultät für Mathematik

Universitätsstr. 25, 33615 Bielefeld, Germany

E-mail: {baeumer,cai}@math.uni-bielefeld.de

In cooperation with:

Harout Aydinian

Vladimir Blinovsky *

Christian Deppe

Haik Mashurian

Universität Bielefeld, Fakultät für Mathematik

Universitätsstr. 25, 33615 Bielefeld, Germany

E-mail: {ayd,cdeppe,hmashur}@math.uni-bielefeld.de

* Russian Academy of Sciences

Institute of Problems of Information Transmission

Bol'shoi Karetnyi per. 19, 101447 Moscow, Russia

E-mail: blinov@postman.ru

Library of Congress Control Number: 2006937883

CR Subject Classification (1998): F.2, G.2-3, C.2, G.1.6, E.3-5

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743

ISBN-10 3-540-46244-9 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-46244-6 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2006

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 11889342 06/3142 5 4 3 2 1 0

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Preface

The Center for Interdisciplinary Research (ZiF) of the University of Bielefeld hosted a research group under the title “General Theory of Information Transfer and Combinatorics,” abbreviated as GTIT-C, from October 1, 2001 to September 30, 2004. As head of the research group the editor shaped the group’s scientific directions and its personal composition.

He followed ideas, problems and results which had occupied him during the past decade and which seem to extend the frontiers of information theory in several directions. The main contributions concern information transfer by channels. There are also new questions and some answers in new models of source coding. While many of the investigations are in an explorative state, there are also hard cores of mathematical theories. In particular, a unified theory of information transfer was presented, which naturally incorporates Shannon’s Theory of Information Transmission and the Theory of Identification in the presence of noise as extremal cases. It provides several novel coding theorems. On the source coding side the concept of identification entropy is introduced. Finally, beyond information theory new concepts of solutions for probabilistic algorithms arose.

In addition to this book there will be a special issue of *Discrete Applied Mathematics* “General Theory of Information Transfer and Combinatorics” in three parts, which covers primarily work with a stronger emphasis on the second component, combinatorics. It begins with an updated version of “General Theory of Information Transfer” in order to make the theory known to a broader audience and continues with other new directions such as bioinformatics, search, sorting and ordering, cryptology and number theory, and networks with many new suggestions for connections.

It includes in a special volume works and abstracts of lectures devoted to the great Levon Khachatrian at the memorial held for him during the Opening Conference, November 4-9, 2002.

In a preparatory year, October 1, 2001 – September 30, 2002, guided by the general concepts and ideas indicated and described in greater detail in the present introduction, researchers and research institutions were approached worldwide in order to find out which possible participants might be and which more concrete projects could be realized in the main research year, October 1, 2002 to August 31, 2003.

Central events in this phase were two weekly preparatory meetings in February: General Theory of Information Transfer, abbreviated as GTIT, and Information in Natural Sciences, Social Sciences, Humanities and Engineering. Abstracts of the lectures can be found at

<http://www.math.uni-bielefeld.de/ahlsweide/zif>.

The main goals were to test the applicability of the GTIT, particularly identification, and to strive for new information phenomena in the sciences, which

can be modelled mathematically. Readers are strongly advised to read the Introduction for guidance.

Our special thanks go to the members of the administration of the “Zentrum für interdisziplinäre Forschung” (ZiF) in Bielefeld for a very pleasant cooperation and, in particular, to Gertrude Lübke-Wolf, who as acting director authorized and generously supported this project, and to Ibke Wachsmuth, who continued her policy. Dr. Roggenhöfer, who was always responsive to new ideas and wishes is also thanked for his assistance.

June 2006

Rudolf Ahlswede

Lecture Notes in Computer Science

For information about Vols. 1–4238

please contact your bookseller or Springer

- Vol. 4345: N. Maglaveras, I. Chouvarda, V. Koutkias, R.W. Brause (Eds.), *Biological and Medical Data Analysis*. XIII, 496 pages. 2006. (Sublibrary LNBI).
- Vol. 4338: P. Kalra, S. Peleg (Eds.), *Computer Vision, Graphics and Image Processing*. XV, 965 pages. 2006.
- Vol. 4337: S. Arun-Kumar, N. Garg (Eds.), *FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science*. XIII, 430 pages. 2006.
- Vol. 4333: U. Reimer, D. Karagiannis (Eds.), *Practical Aspects of Knowledge Management*. XII, 338 pages. 2006. (Sublibrary LNAI).
- Vol. 4331: G. Min, B. Di Martino, L.T. Yang, M. Guo, G. Ruenger (Eds.), *Frontiers of High Performance Computing and Networking – ISPA 2006 Workshops*. XXXVII, 1141 pages. 2006.
- Vol. 4329: R. Barua, T. Lange (Eds.), *Progress in Cryptology – INDOCRYPT 2006*. X, 454 pages. 2006.
- Vol. 4326: S. Göbel, R. Malkewitz, I. Iurgel (Eds.), *Technologies for Interactive Digital Storytelling and Entertainment*. X, 384 pages. 2006.
- Vol. 4325: J. Cao, I. Stojmenovic, X. Jia, S.K. Das (Eds.), *Mobile Ad-hoc and Sensor Networks*. XIX, 887 pages. 2006.
- Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), *Information Security and Cryptology*. XI, 305 pages. 2006.
- Vol. 4313: T. Margaria, B. Steffen (Eds.), *Leveraging Applications of Formal Methods*. IX, 197 pages. 2006.
- Vol. 4312: S. Sugimoto, J. Hunter, A. Rauber, A. Morishima (Eds.), *Digital Libraries: Achievements, Challenges and Opportunities*. XVIII, 571 pages. 2006.
- Vol. 4311: K. Cho, P. Jacquet (Eds.), *Technologies for Advanced Heterogeneous Networks II*. XI, 253 pages. 2006.
- Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), *Information and Communications Security*. XIV, 558 pages. 2006.
- Vol. 4306: Y. Avrithis, Y. Kompatsiaris, S. Staab, N.E. O'Connor (Eds.), *Semantic Multimedia*. XII, 241 pages. 2006.
- Vol. 4305: A.A. Shvartsman (Ed.), *Principles of Distributed Systems*. XIII, 441 pages. 2006.
- Vol. 4304: A. Sattar, B.-H. Kang (Eds.), *AI 2006: Advances in Artificial Intelligence*. XXVII, 1303 pages. 2006. (Sublibrary LNAI).
- Vol. 4302: J. Domingo-Ferrer, L. Franconi (Eds.), *Privacy in Statistical Databases*. XI, 383 pages. 2006.
- Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), *Cryptography and Network Security*. XIII, 381 pages. 2006.
- Vol. 4300: Y.Q. Shi (Ed.), *Transactions on Data Hiding and Multimedia Security I*. IX, 139 pages. 2006.
- Vol. 4296: M.S. Rhee, B. Lee (Eds.), *Information Security and Cryptology – ICISC*. XIII, 358 pages. 2006.
- Vol. 4295: J.D. Carswell, T. Tezuka (Eds.), *Web and Wireless Geographical Information Systems*. XI, 269 pages. 2006.
- Vol. 4294: A. Dan, W. Lamersdorf (Eds.), *Service-Oriented Computing – ICSOC 2006*. XIX, 653 pages. 2006.
- Vol. 4293: A. Gelbukh, C.A. Reyes-Garcia (Eds.), *MICA1 2006: Advances in Artificial Intelligence*. XXVIII, 1232 pages. 2006. (Sublibrary LNAI).
- Vol. 4292: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), *Advances in Visual Computing, Part II*. XXXII, 906 pages. 2006.
- Vol. 4291: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), *Advances in Visual Computing, Part I*. XXXI, 916 pages. 2006.
- Vol. 4290: M. van Steen, M. Henning (Eds.), *Middleware 2006*. XIII, 425 pages. 2006.
- Vol. 4289: M. Ackermann, B. Berendt, M. Grobelnik, A. Hotho, D. Mladenich, G. Semeraro, M. Spiliopoulou, G. Stumme, V. Svatek, M. van Someren (Eds.), *Semantics, Web and Mining*. X, 197 pages. 2006. (Sublibrary LNAI).
- Vol. 4288: T. Asano (Ed.), *Algorithms and Computation*. XX, 766 pages. 2006.
- Vol. 4286: P. Spirakis, M. Mavronicolas, S. Kontogiannis (Eds.), *Internet and Network Economics*. XI, 401 pages. 2006.
- Vol. 4285: Y. Matsumoto, R. Sproat, K.-F. Wong, M. Zhang (Eds.), *Computer Processing of Oriental Languages*. XVII, 544 pages. 2006. (Sublibrary LNAI).
- Vol. 4284: X. Lai, K. Chen (Eds.), *Advances in Cryptology – ASIACRYPT 2006*. XIV, 468 pages. 2006.
- Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), *Digital Watermarking*. XII, 474 pages. 2006.
- Vol. 4282: Z. Pan, A. Cheok, M. Haller, R.W.H. Lau, H. Saito, R. Liang (Eds.), *Advances in Artificial Reality and Tele-Existence*. XXIII, 1347 pages. 2006.
- Vol. 4281: K. Barkaoui, A. Cavalcanti, A. Cerone (Eds.), *Theoretical Aspects of Computing – ICTAC 2006*. XV, 371 pages. 2006.
- Vol. 4280: A.K. Datta, M. Gradinariu (Eds.), *Stabilization, Safety, and Security of Distributed Systems*. XVII, 590 pages. 2006.

- Vol. 4279: N. Kobayashi (Ed.), *Programming Languages and Systems*. XI, 423 pages. 2006.
- Vol. 4278: R. Meersman, Z. Tari, P. Herrero (Eds.), *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Part II*. XLV, 1004 pages. 2006.
- Vol. 4277: R. Meersman, Z. Tari, P. Herrero (Eds.), *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Part I*. XLV, 1009 pages. 2006.
- Vol. 4276: R. Meersman, Z. Tari (Eds.), *On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part II*. XXXII, 752 pages. 2006.
- Vol. 4275: R. Meersman, Z. Tari (Eds.), *On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part I*. XXXI, 1115 pages. 2006.
- Vol. 4274: Q. Huo, B. Ma, E.-S. Chng, H. Li (Eds.), *Chinese Spoken Language Processing*. XXIV, 805 pages. 2006. (Sublibrary LNAI).
- Vol. 4273: I. Cruz, S. Decker, D. Allemang, C. Preist, D. Schwabe, P. Mika, M. Uschold, L. Aroyo (Eds.), *The Semantic Web - ISWC 2006*. XXIV, 1001 pages. 2006.
- Vol. 4272: P. Havinga, M. Lijding, N. Meratnia, M. Wegdam (Eds.), *Smart Sensing and Context*. XI, 267 pages. 2006.
- Vol. 4271: F.V. Fomin (Ed.), *Graph-Theoretic Concepts in Computer Science*. XIII, 358 pages. 2006.
- Vol. 4270: H. Zha, Z. Pan, H. Thwaites, A.C. Addison, M. Forte (Eds.), *Interactive Technologies and Sociotechnical Systems*. XVI, 547 pages. 2006.
- Vol. 4269: R. State, S. van der Meer, D. O'Sullivan, T. Pfeifer (Eds.), *Large Scale Management of Distributed Systems*. XIII, 282 pages. 2006.
- Vol. 4268: G. Parr, D. Malone, M. Ó Foghlú (Eds.), *Autonomic Principles of IP Operations and Management*. XIII, 237 pages. 2006.
- Vol. 4267: A. Helmy, B. Jennings, L. Murphy, T. Pfeifer (Eds.), *Autonomic Management of Mobile Multimedia Services*. XIII, 257 pages. 2006.
- Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenber, Y. Murayama, S. Kawamura (Eds.), *Advances in Information and Computer Security*. XIII, 438 pages. 2006.
- Vol. 4265: L. Todorovski, N. Lavrač, K.P. Jantke (Eds.), *Discovery Science*. XIV, 384 pages. 2006. (Sublibrary LNAI).
- Vol. 4264: J.L. Balcázar, P.M. Long, F. Stephan (Eds.), *Algorithmic Learning Theory*. XIII, 393 pages. 2006. (Sublibrary LNAI).
- Vol. 4263: A. Levi, E. Savaş, H. Yenigün, S. Balcisoy, Y. Saygın (Eds.), *Computer and Information Sciences - ISCIS 2006*. XXIII, 1084 pages. 2006.
- Vol. 4262: K. Havelund, M. Núñez, B. Wolff, G. Roşu (Eds.), *Formal Approaches to Software Testing and Runtime Verification*. VIII, 255 pages. 2006.
- Vol. 4261: Y. Zhuang, S. Yang, Y. Rui, Q. He (Eds.), *Advances in Multimedia Information Processing - PCM 2006*. XXII, 1040 pages. 2006.
- Vol. 4260: Z. Liu, J. He (Eds.), *Formal Methods and Software Engineering*. XII, 778 pages. 2006.
- Vol. 4259: S. Greco, Y. Hata, S. Hirano, M. Inuiguchi, S. Miyamoto, H.S. Nguyen, R. Słowiński (Eds.), *Rough Sets and Current Trends in Computing*. XXII, 951 pages. 2006. (Sublibrary LNAI).
- Vol. 4257: I. Richardson, P. Runeson, R. Messnarz (Eds.), *Software Process Improvement*. XI, 219 pages. 2006.
- Vol. 4256: L. Feng, G. Wang, C. Zeng, R. Huang (Eds.), *Web Information Systems - WISE 2006 Workshops*. XIV, 320 pages. 2006.
- Vol. 4255: K. Aberer, Z. Peng, E.A. Rundensteiner, Y. Zhang, X. Li (Eds.), *Web Information Systems - WISE 2006*. XIV, 563 pages. 2006.
- Vol. 4254: T. Grust, H. Höpfner, A. Illarramendi, S. Jablonski, M. Mesiti, S. Müller, P.-L. Patranjan, K.-U. Sattler, M. Spiliopoulou, J. Wijsen (Eds.), *Current Trends in Database Technology - EDBT 2006*. XXXI, 932 pages. 2006.
- Vol. 4253: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), *Knowledge-Based Intelligent Information and Engineering Systems, Part III*. XXXII, 1301 pages. 2006. (Sublibrary LNAI).
- Vol. 4252: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), *Knowledge-Based Intelligent Information and Engineering Systems, Part II*. XXXIII, 1335 pages. 2006. (Sublibrary LNAI).
- Vol. 4251: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), *Knowledge-Based Intelligent Information and Engineering Systems, Part I*. LXVI, 1297 pages. 2006. (Sublibrary LNAI).
- Vol. 4250: H.J. van den Herik, S.-C. Hsu, T.-s. Hsu, H.H.L.M. Donkers (Eds.), *Advances in Computer Games*. XIV, 273 pages. 2006.
- Vol. 4249: L. Goubin, M. Matsui (Eds.), *Cryptographic Hardware and Embedded Systems - CHES 2006*. XII, 462 pages. 2006.
- Vol. 4248: S. Staab, V. Svátek (Eds.), *Managing Knowledge in a World of Networks*. XIV, 400 pages. 2006. (Sublibrary LNAI).
- Vol. 4247: T.-D. Wang, X. Li, S.-H. Chen, X. Wang, H. Abbass, H. Iba, G. Chen, X. Yao (Eds.), *Simulated Evolution and Learning*. XXI, 940 pages. 2006.
- Vol. 4246: M. Hermann, A. Voronkov (Eds.), *Logic for Programming, Artificial Intelligence, and Reasoning*. XIII, 588 pages. 2006. (Sublibrary LNAI).
- Vol. 4245: A. Kuba, L.G. Nyúl, K. Palágyi (Eds.), *Discrete Geometry for Computer Imagery*. XIII, 688 pages. 2006.
- Vol. 4244: S. Spaccapietra (Ed.), *Journal on Data Semantics VII*. XI, 267 pages. 2006.
- Vol. 4243: T. Yakhno, E.J. Neuhold (Eds.), *Advances in Information Systems*. XIII, 420 pages. 2006.
- Vol. 4242: A. Rashid, M. Aksit (Eds.), *Transactions on Aspect-Oriented Software Development II*. IX, 289 pages. 2006.
- Vol. 4241: R.R. Beichel, M. Sonka (Eds.), *Computer Vision Approaches to Medical Image Analysis*. XI, 262 pages. 2006.
- Vol. 4239: H.Y. Youn, M. Kim, H. Morikawa (Eds.), *Ubiquitous Computing Systems*. XVI, 548 pages. 2006.

¥837.00元

Table of Contents

Introduction	1
Rudolf Ahlswede – From 60 to 66	45
Information Theory and Some Friendly Neighbors – Ein Wunschkonzert	49
I Probabilistic Models	
1 Identification for Sources <i>Rudolf Ahlswede, Bernhard Balkenhol, Christian Kleinewächter</i>	51
2 On Identification <i>Christian Kleinewächter</i>	62
3 Identification and Prediction <i>Lars Bäumer</i>	84
4 Watermarking Identification Codes with Related Topics on Common Randomness <i>Rudolf Ahlswede, Ning Cai</i>	107
5 Notes on Conditions for Successive Refinement of Information <i>Ashot N. Harutyunyan</i>	154
6 Coding for the Multiple-Access Adder Channel <i>Bálint Laczay</i>	165
7 Bounds of E -Capacity for Multiple-Access Channel with Random Parameter <i>Mariam E. Haroutunian</i>	196
8 Huge Size Codes for Identification Via a Multiple Access Channel Under a Word-Length Constraint <i>Sándor Csibi, Edward von der Meulen</i>	218
9 Codes with the Identifiable Parent Property and the Multiple-Access Channel <i>Rudolf Ahlswede, Ning Cai</i>	249

II Cryptology – Pseudo Random Sequences

10	Transmission, Identification and Common Randomness Capacities for Wire-Tape Channels with Secure Feedback from the Decoder ...	258
	<i>Rudolf Ahlswede, Ning Cai</i>	
11	A Simplified Method for Computing the Key Equivocation for Additive-Like Instantaneous Block Encipherers	276
	<i>Zhaozhi Zhang</i>	
12	Secrecy Systems for Identification Via Channels with Additive-Like Instantaneous Block Encipherer	285
	<i>Rudolf Ahlswede, Ning Cai, Zhaozhi Zhang</i>	
13	Large Families of Pseudorandom Sequences of k Symbols and Their Complexity – Part I	293
	<i>Rudolf Ahlswede, Christian Mauduit, András Sárközy</i>	
14	Large Families of Pseudorandom Sequences of k Symbols and Their Complexity – Part II	308
	<i>Rudolf Ahlswede, Christian Mauduit, András Sárközy</i>	
15	On a Fast Version of a Pseudorandom Generator	326
	<i>Katalin Gyarmati</i>	
16	On Pseudorandom Sequences and Their Application	343
	<i>Joël Rivat, András Sárközy</i>	
17	Authorship Attribution of Texts: A Review	362
	<i>Mikhail B. Maljutov</i>	

III Quantum Models

18	Raum-Zeit und Quantenphysik – Ein Geburtstagsständchen für Hans-Jürgen Treder	381
	<i>Armin Uhlmann</i>	
19	Quantum Information Transfer from One System to Another One	394
	<i>Armin Uhlmann</i>	
20	On Rank Two Channels	413
	<i>Armin Uhlmann</i>	
21	Universal Sets of Quantum Information Processing Primitives and Their Optimal Use	425
	<i>Jożef Gruska</i>	

22	An Upper Bound on the Rate of Information Transfer by Grover's Oracle	452
	<i>Erdal Arıkan</i>	
23	A Strong Converse Theorem for Quantum Multiple Access Channels	460
	<i>Rudolf Ahlswede, Ning Cai</i>	
24	Identification Via Quantum Channels in the Presence of Prior Correlation and Feedback	486
	<i>Andreas Winter</i>	
25	Additive Number Theory and the Ring of Quantum Integers	505
	<i>Melvyn B. Nathanson</i>	
26	The Proper Fiducial Argument	512
	<i>Frank Hampel</i>	
27	On Sequential Discrimination Between Close Markov Chains	527
	<i>Mikhail B. Malyutov, Dmitry M. Malyutov</i>	
28	Estimating with Randomized Encoding the Joint Empirical Distribution in a Correlated Source	535
	<i>Rudolf Ahlswede, Zhen Zhang</i>	
29	On Logarithmically Asymptotically Optimal Hypothesis Testing for Arbitrarily Varying Sources with Side Information	547
	<i>Rudolf Ahlswede, Ella Aloyan, Evgueni Haroutunian</i>	
30	On Logarithmically Asymptotically Optimal Testing of Hypotheses and Identification	553
	<i>Rudolf Ahlswede, Evgueni Haroutunian</i>	
31	Correlation Inequalities in Function Spaces	572
	<i>Rudolf Ahlswede, Vladimir Blinovsky</i>	
32	Lower Bounds for Divergence in the Central Limit Theorem	578
	<i>Peter Harremoës</i>	
 V Information Measures – Error Concepts – Performance Criteria		
33	Identification Entropy	595
	<i>Rudolf Ahlswede</i>	
34	Optimal Information Measures for Weakly Chaotic Dynamical Systems	614
	<i>Vieri Benci, Stefano Galatolo</i>	

35	Report on Models of Write-Efficient Memories with Localized Errors and Defects	628
	<i>Rudolf Ahlswede, Mark S. Pinsker</i>	
36	Percolation on a k -Ary Tree	633
	<i>Kingo Kobayashi, Hiroyoshi Morita, Mamoru Hoshi</i>	
37	On Concepts of Performance Parameters for Channels	639
	<i>Rudolf Ahlswede</i>	
38	Appendix: On Common Information and Related Characteristics of Correlated Information Sources	664
	<i>Rudolf Ahlswede, Janos Körner</i>	

VI Search – Sorting – Ordering – Planning

39	Q -Ary Ulam-Renyi Game with Constrained Lies	678
	<i>Ferdinando Cicalese, Christian Deppe</i>	
40	Search with Noisy and Delayed Responses	695
	<i>Rudolf Ahlswede, Ning Cai</i>	
41	A Kraft-Type Inequality for d -Delay Binary Search Codes	704
	<i>Rudolf Ahlswede, Ning Cai</i>	
42	Threshold Group Testing	707
	<i>Peter Damaschke</i>	
43	A Fast Suffix-Sorting Algorithm	719
	<i>Rudolf Ahlswede, Bernhard Balkenhol, Christian Deppe, Martin Fröhlich</i>	
44	Monotonicity Checking	735
	<i>Marina Kyureghyan</i>	
45	Algorithmic Motion Planning: The Randomized Approach	740
	<i>Stefano Carpin</i>	

VII Language Evolution – Pattern Discovery – Reconstructions

46	Information Theoretic Models in Language Evolution	769
	<i>Rudolf Ahlswede, Erdal Arıkan, Lars Bäumer, Christian Deppe</i>	
47	Zipf's Law, Hyperbolic Distributions and Entropy Loss	788
	<i>Peter Harremoës, Flemming Topsøe</i>	

48	Bridging Lossy and Lossless Compression by Motif Pattern Discovery	793
	<i>Alberto Apostolico, Matteo Comin, Laxmi Parida</i>	
49	Reverse-Complement Similarity Codes	814
	<i>Arkadii D'yachkov, David Torney, Pavel Vilenkin, Scott White</i>	
50	On Some Applications of Information Indices in Chemical Graph Theory	831
	<i>Elena V. Konstantinova</i>	
51	Largest Graphs of Diameter 2 and Maximum Degree 6	853
	<i>Sergey G. Molodtsov</i>	

VIII Network Coding

52	An Outside Opinion	858
	<i>Rudolf Ahlswede</i>	
53	Problems in Network Coding and Error Correcting Codes Appended by a Draft Version of S. Riis "Utilising Public Information in Network Coding"	861
	<i>Soren Riis, Rudolf Ahlswede</i>	

IX Combinatorial Models

Coverings

54	On the Thinnest Coverings of Spheres and Ellipsoids with Balls in Hamming and Euclidean Spaces	898
	<i>Ilya Dumer, Mark S. Pinsker, Viacheslav V. Prelov</i>	
55	Appendix: On Set Coverings in Cartesian Product Spaces	926
	<i>Rudolf Ahlswede</i>	

Partitions

56	Testing Sets for 1-Perfect Code	938
	<i>Sergey V. Augustinovich, Anastasia Yu. Vasil'eva</i>	
57	On Partitions of a Rectangle into Rectangles with Restricted Number of Cross Sections	941
	<i>Rudolf Ahlswede, Alexander A. Yudin</i>	

Isoperimetry

58	On Attractive and Friendly Sets in Sequence Spaces	955
	<i>Rudolf Ahlswede, Levon Khachatrian</i>	

59	Remarks on an Edge Isoperimetric Problem	971
	<i>Christian Bey</i>	

60	Appendix: On Edge–Isoperimetric Theorems for Uniform Hypergraphs	979
	<i>Rudolf Ahlswede, Ning Cai</i>	

Isodiametry

61	Appendix: Solution of Burnashev’s Problem and a Sharpening of the Erdős/Ko/Rado Theorem	1006
	<i>Rudolf Ahlswede</i>	

Networks

62	Realization of Intensity Modulated Radiation Fields Using Multileaf Collimators	1010
	<i>Thomas Kalinowski</i>	

63	Sparse Asymmetric Connectors in Communication Networks	1056
	<i>Rudolf Ahlswede, Harout Aydinian</i>	

X Problem Section

64	Finding $C_{\text{NRI}}(\mathcal{W})$, the Identification Capacity of the AVC $\mathcal{W}$, if Randomization in the Encoding Is Excluded	1063
	<i>Rudolf Ahlswede</i>	

65	Intersection Graphs of Rectangles and Segments	1064
	<i>Rudolf Ahlswede, Iskandar Karapetyan</i>	

66	Cutoff Rate Enhancement	1066
	<i>Erdal Arıkan</i>	

67	Some Problems in Organic Coding Theory	1069
	<i>Stefan Artmann</i>	

68	Generalized Anticodes in Hamming Spaces	1073
	<i>Harout Aydinian</i>	

69	Two Problems from Coding Theory	1075
	<i>Vladimir Blinovskiy</i>	

70	Private Capacity of Broadcast Channels	1076
	<i>Ning Cai</i>	

71	A Short Survey on Upper and Lower Bounds for Multidimensional Zero Sums	1079
	<i>Christian Elsholtz</i>	

72	Binary Linear Codes That Are Optimal for Error Correction	1081
	<i>Torleiv Kløve</i>	
73	Capacity Problem of Trapdoor Channel	1084
	<i>Kingo Kobayashi</i>	
74	Hotlink Assignment on the Web	1088
	<i>Eduardo Sany Laber</i>	
75	The Rigidity of Hamming Spaces	1093
	<i>Vasilij S. Lebedev</i>	
76	A Conjecture in Finite Fields	1095
	<i>Uwe Leck</i>	
77	Multiparty Computations in Non-private Environments	1097
	<i>Maciej Liśkiewicz</i>	
78	Some Mathematical Problems Related to Quantum Hypothesis Testing	1100
	<i>Hiroshi Nagaoka</i>	
79	Designs and Perfect Codes	1104
	<i>Faina I. Solov'eva</i>	
80	Special Issue of Discrete Applied Mathematics: "General Theory of Information Transfer and Combinatorics" List D	1106
81	Bibliography of Publications by Rudolf Ahlswede	1109
	<i>Rudolf Ahlswede</i>	
	Author Index	1125

Addresses of Contributors to the Project as well as Titles and Abstracts of their lectures delivered at two Preparatory Meetings, the Opening Conference, the Final Meeting and Seminars the Reader can find at <http://www.math.uni-bielefeld.de/ahlsweide/zif>

More than restoring
strings of symbols transmitted
means transfer today

Rudolf Ahlswede

Introduction



The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.

Claude E. Shannon

What is information?

Cn bits in Shannon's fundamental theorem

or

$\log Cn$ bits in our Theory of Identification ?

Among the directions of research in GTIT-C, which could be established, we present in Chapters I-IX contributions of participants, which took shape in written form. The papers were thoroughly refereed. For the ease of reference they are numbered and in addition labelled by the letter B, which hints at this book.

There are other lists of publications we refer to. They are labelled by A,C, and D, where

- A indicates the editors present list of publications at the end of the book
- C is used for papers mentioned in the preface, in particular in these comments
- D gives the titles of the papers in the related Special Issue in Discrete Applied Mathematics (3 volumes)

It must be emphasized that there were several lectures and discussions with many ideas, which influenced work, which appears elsewhere. Also, several subjects with noticeable informational components are not ready for a theoretical and in particular mathematical frame.

For instance in **Bio-Chemistry** there are many advanced experiments concerning “signalling”, where some kind of intensity is measured, but essentially nothing is known about transmission rates. Still we learnt a lot from several very stimulating lectures of Raimund Apfelbach about the “state of the art”. Moreover, we are particularly thankful for his engagement in helping to shape a group for **Animal Communication** beyond his own work related to smelling.

In many lectures, especially also by young German emigrants to Great Britain, we were excited by an extremely rich and very active field in recent years. There are fascinating ways of encoding information (well-known a long time for bees and more recently for ants etc). Mathematical models are more in a beginning state. Our hope that in the kingdom of animals nature has chosen other forms of information transfer, like in identification, could not be verified. It seems that knowledge of these forms is a necessary prerequisite for setting up suitable experiments.

At least we know where one may start. Several abstracts from the April 2004 Final Meeting the reader can find at

<http://www.math.uni-bielefeld.de/ahlsweide/zif>. We also mention two instructive books [C10], [C49]. With advanced technology many new experiments have become possible here.

Similar observations can be made about **Psychology**. However, there have been signals encouraging careful reading, intuitive perception or enjoyment of G. Dueck’s book [C25] with its classification of people into “right”, “true” or “natural” and corresponding different key roles identification seems to play for them.

A last statement in this context we want to make about **Philosophical Ideas** concerning *information concepts and measures*, in particular about K.F. von Weizsäcker’s monumental *attempt* [C100] to base all of Physics on an information concept – central even for time and space. We found that the newly discovered concept of *identification entropy* [B33], which has an unquestionable operational meaning, *is not covered by that approach and therefore challenges it!* Philosophers are called again to share a world with mathematicians and vice versa.

We hope to have made understandable why we did not receive contributions to Bio-Chemistry, Animal Communication, Psychology and Philosophy for this book.

There is, however, for instance a contribution to **Language Evolution** [B46], in which a **Conjecture of Nowak**, the man who has been running a five year