Lecture Notes in Computer Science 4123

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

Rudolf Ahlswede
Lars Bäumer Ning Cai
Harout Aydinian Vladimir Blinovsky
Christian Deppe Haik Mashurian (Eds.)

General Theory of Information Transfer and Combinatorics

Springer

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

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/ahlswede/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 Lübbe-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

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 51
Rudolf Ahlswede, Bernhard Balkenhol, Christian Kleinewächter

2 On Identification 62
Christian Kleinewächter

3 Identification and Prediction 84
Lars Bäumer

4 Watermarking Identification Codes with Related Topics on Common Randomness 107
Rudolf Ahlswede, Ning Cai

5 Notes on Conditions for Successive Refinement of Information 154
Ashot N. Harutyunyan

6 Coding for the Multiple-Access Adder Channel 165
Bálint Laczay

7 Bounds of E-Capacity for Multiple-Access Channel with Random Parameter 196
Mariam E. Haroutunian

8 Huge Size Codes for Identification Via a Multiple Access Channel Under a Word-Length Constraint 218
Sándor Csibi, Edward von der Meulen

9 Codes with the Identifiable Parent Property and the Multiple-Access Channel 249
Rudolf Ahlswede, Ning Cai

II Cryptology – Pseudo Random Sequences

10 Transmission, Identification and Common Randomness Capacities for Wire-Tape Channels with Secure Feedback from the Decoder ... 258
Rudolf Ahlswede, Ning Cai

11 A Simplified Method for Computing the Key Equivocation for Additive-Like Instantaneous Block Encipherers ... 276
Zhaozhi Zhang

12 Secrecy Systems for Identification Via Channels with Additive-Like Instantaneous Block Encipherer ... 285
Rudolf Ahlswede, Ning Cai, Zhaozhi Zhang

13 Large Families of Pseudorandom Sequences of k Symbols and Their Complexity – Part I ... 293
Rudolf Ahlswede, Christian Mauduit, András Sárközy

14 Large Families of Pseudorandom Sequences of k Symbols and Their Complexity – Part II ... 308
Rudolf Ahlswede, Christian Mauduit, András Sárközy

15 On a Fast Version of a Pseudorandom Generator ... 326
Katalin Gyarmati

16 On Pseudorandom Sequences and Their Application ... 343
Joël Rivat, András Sárközy

17 Authorship Attribution of Texts: A Review ... 362
Mikhail B. Malyutov

III Quantum Models

18 Raum-Zeit und Quantenphysik – Ein Geburtstagsständchen für Hans-Jürgen Treder ... 381
Armin Uhlmann

19 Quantum Information Transfer from One System to Another One ... 394
Armin Uhlmann

20 On Rank Two Channels ... 413
Armin Uhlmann

21 Universal Sets of Quantum Information Processing Primitives and Their Optimal Use ... 425
Jozef Gruska

22 An Upper Bound on the Rate of Information Transfer by Grover's Oracle 452
Erdal Arikan

23 A Strong Converse Theorem for Quantum Multiple Access Channels 460
Rudolf Ahlswede, Ning Cai

24 Identification Via Quantum Channels in the Presence of Prior Correlation and Feedback 486
Andreas Winter

25 Additive Number Theory and the Ring of Quantum Integers 505
Melvyn B. Nathanson

26 The Proper Fiducial Argument 512
Frank Hampel

27 On Sequential Discrimination Between Close Markov Chains 527
Mikhail B. Malyutov, Dmitry M. Malyutov

28 Estimating with Randomized Encoding the Joint Empirical Distribution in a Correlated Source 535
Rudolf Ahlswede, Zhen Zhang

29 On Logarithmically Asymptotically Optimal Hypothesis Testing for Arbitrarily Varying Sources with Side Information 547
Rudolf Ahlswede, Ella Aloyan, Evgueni Haroutunian

30 On Logarithmically Asymptotically Optimal Testing of Hypotheses and Identification 553
Rudolf Ahlswede, Evgueni Haroutunian

31 Correlation Inequalities in Function Spaces 572
Rudolf Ahlswede, Vladimir Blinovsky

32 Lower Bounds for Divergence in the Central Limit Theorem 578
Peter Harremoës

V Information Measures – Error Concepts – Performance Criteria

33 Identification Entropy 595
Rudolf Ahlswede

34 Optimal Information Measures for Weakly Chaotic Dynamical Systems 614
Vieri Benci, Stefano Galatolo

35 Report on Models of Write–Efficient Memories with Localized Errors and Defects 628
Rudolf Ahlswede, Mark S. Pinsker

36 Percolation on a k-Ary Tree 633
Kingo Kobayashi, Hiroyoshi Morita, Mamoru Hoshi

37 On Concepts of Performance Parameters for Channels 639
Rudolf Ahlswede

38 Appendix: On Common Information and Related Characteristics of Correlated Information Sources 664
Rudolf Ahlswede, Janos Körner

VI Search – Sorting – Ordering – Planning

39 Q-Ary Ulam-Renyi Game with Constrained Lies 678
Ferdinando Cicalese, Christian Deppe

40 Search with Noisy and Delayed Responses 695
Rudolf Ahlswede, Ning Cai

41 A Kraft–Type Inequality for d–Delay Binary Search Codes 704
Rudolf Ahlswede, Ning Cai

42 Threshold Group Testing 707
Peter Damaschke

43 A Fast Suffix-Sorting Algorithm 719
Rudolf Ahlswede, Bernhard Balkenhol, Christian Deppe, Martin Fröhlich

44 Monotonicity Checking 735
Marina Kyureghyan

45 Algorithmic Motion Planning: The Randomized Approach 740
Stefano Carpin

VII Language Evolution – Pattern Discovery – Reconstructions

46 Information Theoretic Models in Language Evolution 769
Rudolf Ahlswede, Erdal Arikan, Lars Bäumer, Christian Deppe

47 Zipf's Law, Hyperbolic Distributions and Entropy Loss 788
Peter Harremoës, Flemming Topsoe

48 Bridging Lossy and Lossless Compression by Motif Pattern Discovery 793
Alberto Apostolico, Matteo Comin, Laxmi Parida

49 Reverse–Complement Similarity Codes 814
Arkadii D'yachkov, David Torney, Pavel Vilenkin, Scott White

50 On Some Applications of Information Indices in Chemical Graph Theory 831
Elena V. Konstantinova

51 Largest Graphs of Diameter 2 and Maximum Degree 6 853
Sergey G. Molodtsov

VIII Network Coding

52 An Outside Opinion 858
Rudolf Ahlswede

53 Problems in Network Coding and Error Correcting Codes Appended by a Draft Version of S. Riis "Utilising Public Information in Network Coding" 861
Soren Riis, Rudolf Ahlswede

IX Combinatorial Models

Coverings

54 On the Thinnest Coverings of Spheres and Ellipsoids with Balls in Hamming and Euclidean Spaces 898
Ilya Dumer, Mark S. Pinsker, Viacheslav V. Prelov

55 Appendix: On Set Coverings in Cartesian Product Spaces 926
Rudolf Ahlswede

Partitions

56 Testing Sets for 1-Perfect Code 938
Sergey V. Avgustinovich, Anastasia Yu. Vasil'eva

57 On Partitions of a Rectangle into Rectangles with Restricted Number of Cross Sections 941
Rudolf Ahlswede, Alexander A. Yudin

Isoperimetry

58 On Attractive and Friendly Sets in Sequence Spaces 955
Rudolf Ahlswede, Levon Khachatrian

59 Remarks on an Edge Isoperimetric Problem 971
Christian Bey

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

Isodiametry

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

Networks

62 Realization of Intensity Modulated Radiation Fields Using Multileaf Collimators 1010
Thomas Kalinowski

63 Sparse Asymmetric Connectors in Communication Networks 1056
Rudolf Ahlswede, Harout Aydinian

X Problem Section

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

65 Intersection Graphs of Rectangles and Segments 1064
Rudolf Ahlswede, Iskandar Karapetyan

66 Cutoff Rate Enhancement 1066
Erdal Arikan

67 Some Problems in Organic Coding Theory 1069
Stefan Artmann

68 Generalized Anticodes in Hamming Spaces 1073
Harout Aydinian

69 Two Problems from Coding Theory 1075
Vladimir Blinovsky

70 Private Capacity of Broadcast Channels 1076
Ning Cai

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

72 Binary Linear Codes That Are Optimal for Error Correction 1081
Torleiv Kløve

73 Capacity Problem of Trapdoor Channel 1084
Kingo Kobayashi

74 Hotlink Assignment on the Web 1088
Eduardo Sany Laber

75 The Rigidity of Hamming Spaces 1093
Vasilij S. Lebedev

76 A Conjecture in Finite Fields 1095
Uwe Leck

77 Multiparty Computations in Non-private Environments............ 1097
Maciej Liśkiewicz

78 Some Mathematical Problems Related to Quantum Hypothesis Testing.. 1100
Hiroshi Nagaoka

79 Designs and Perfect Codes 1104
Faina I. Solov'eva

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
Rudolf Ahlswede

Author Index 1125

Addresses of Contributers 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/ahlswede/zif`