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

General Theory of Information Transfer and Combinatorics
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 In-
roduction 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 Laczy*

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*
## Table of Contents

### 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*
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Author(s)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>An Upper Bound on the Rate of Information Transfer by Grover’s Oracle</td>
<td>Erdal Arikan</td>
<td>452</td>
</tr>
<tr>
<td>23</td>
<td>A Strong Converse Theorem for Quantum Multiple Access Channels</td>
<td>Rudolf Ahlswede, Ning Cai</td>
<td>460</td>
</tr>
<tr>
<td>24</td>
<td>Identification Via Quantum Channels in the Presence of Prior Correlation and Feedback</td>
<td>Andreas Winter</td>
<td>486</td>
</tr>
<tr>
<td>25</td>
<td>Additive Number Theory and the Ring of Quantum Integers</td>
<td>Melvyn B. Nathanson</td>
<td>505</td>
</tr>
<tr>
<td>26</td>
<td>The Proper Fiducial Argument</td>
<td>Frank Hampel</td>
<td>512</td>
</tr>
<tr>
<td>27</td>
<td>On Sequential Discrimination Between Close Markov Chains</td>
<td>Mikhail B. Malyutov, Dmitry M. Malyutov</td>
<td>527</td>
</tr>
<tr>
<td>28</td>
<td>Estimating with Randomized Encoding the Joint Empirical Distribution in a Correlated Source</td>
<td>Rudolf Ahlswede, Zhen Zhang</td>
<td>535</td>
</tr>
<tr>
<td>29</td>
<td>On Logarithmically Asymptotically Optimal Hypothesis Testing for Arbitrarily Varying Sources with Side Information</td>
<td>Rudolf Ahlswede, Ella Aloyan, Evgueni Haroutunian</td>
<td>547</td>
</tr>
<tr>
<td>30</td>
<td>On Logarithmically Asymptotically Optimal Testing of Hypotheses and Identification</td>
<td>Rudolf Ahlswede, Evgueni Haroutunian</td>
<td>553</td>
</tr>
<tr>
<td>31</td>
<td>Correlation Inequalities in Function Spaces</td>
<td>Rudolf Ahlswede, Vladimir Blinovsky</td>
<td>572</td>
</tr>
<tr>
<td>32</td>
<td>Lower Bounds for Divergence in the Central Limit Theorem</td>
<td>Peter Harremoës</td>
<td>578</td>
</tr>
</tbody>
</table>

V Information Measures – Error Concepts – Performance Criteria

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Author(s)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>Identification Entropy</td>
<td>Rudolf Ahlswede</td>
<td>595</td>
</tr>
<tr>
<td>34</td>
<td>Optimal Information Measures for Weakly Chaotic Dynamical Systems</td>
<td>Vieri Benci, Stefano Galatolo</td>
<td>614</td>
</tr>
</tbody>
</table>
X Table of Contents

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
<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Authors</th>
<th>End Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>59</td>
<td>Remarks on an Edge Isoperimetric Problem</td>
<td>Christian Bey</td>
<td>971</td>
</tr>
<tr>
<td>60</td>
<td>Appendix: On Edge–Isoperimetric Theorems for Uniform Hypergraphs</td>
<td>Rudolf Ahlswede, Ning Cai</td>
<td>979</td>
</tr>
<tr>
<td>61</td>
<td>Appendix: Solution of Burnashev’s Problem and a Sharpening of the Erdős/Ko/Rado Theorem</td>
<td>Rudolf Ahlswede</td>
<td>1006</td>
</tr>
<tr>
<td>62</td>
<td>Realization of Intensity Modulated Radiation Fields Using Multileaf Collimators</td>
<td>Thomas Kalinowski</td>
<td>1010</td>
</tr>
<tr>
<td>63</td>
<td>Sparse Asymmetric Connectors in Communication Networks</td>
<td>Rudolf Ahlswede, Harout Aydinian</td>
<td>1056</td>
</tr>
<tr>
<td>64</td>
<td>Finding $C_{\text{NRI}}(W)$, the Identification Capacity of the AVC $W$, if Randomization in the Encoding Is Excluded</td>
<td>Rudolf Ahlswede</td>
<td>1063</td>
</tr>
<tr>
<td>65</td>
<td>Intersection Graphs of Rectangles and Segments</td>
<td>Rudolf Ahlswede, Iskandar Karapetyan</td>
<td>1064</td>
</tr>
<tr>
<td>66</td>
<td>Cutoff Rate Enhancement</td>
<td>Erdal Arikan</td>
<td>1066</td>
</tr>
<tr>
<td>67</td>
<td>Some Problems in Organic Coding Theory</td>
<td>Stefan Artmann</td>
<td>1069</td>
</tr>
<tr>
<td>68</td>
<td>Generalized Anticodes in Hamming Spaces</td>
<td>Harout Aydinian</td>
<td>1073</td>
</tr>
<tr>
<td>69</td>
<td>Two Problems from Coding Theory</td>
<td>Vladimir Blinovsky</td>
<td>1075</td>
</tr>
<tr>
<td>70</td>
<td>Private Capacity of Broadcast Channels</td>
<td>Ning Cai</td>
<td>1076</td>
</tr>
<tr>
<td>71</td>
<td>A Short Survey on Upper and Lower Bounds for Multidimensional Zero Sums</td>
<td>Christian Elsholtz</td>
<td>1079</td>
</tr>
<tr>
<td>Article Number</td>
<td>Title</td>
<td>Author(s)</td>
<td>Page</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>72</td>
<td>Binary Linear Codes That Are Optimal for Error Correction</td>
<td>Torleiv Kløve</td>
<td>1081</td>
</tr>
<tr>
<td>73</td>
<td>Capacity Problem of Trapdoor Channel</td>
<td>Kingo Kobayashi</td>
<td>1084</td>
</tr>
<tr>
<td>74</td>
<td>Hotlink Assignment on the Web</td>
<td>Eduardo Sany Laber</td>
<td>1088</td>
</tr>
<tr>
<td>75</td>
<td>The Rigidity of Hamming Spaces</td>
<td>Vasilij S. Lebedev</td>
<td>1093</td>
</tr>
<tr>
<td>76</td>
<td>A Conjecture in Finite Fields</td>
<td>Uwe Leck</td>
<td>1095</td>
</tr>
<tr>
<td>77</td>
<td>Multiparty Computations in Non-private Environments</td>
<td>Maciej Liśkiewicz</td>
<td>1097</td>
</tr>
<tr>
<td>78</td>
<td>Some Mathematical Problems Related to Quantum Hypothesis Testing</td>
<td>Hiroshi Nagaoka</td>
<td>1100</td>
</tr>
<tr>
<td>79</td>
<td>Designs and Perfect Codes</td>
<td>Faina I. Solov’eva</td>
<td>1104</td>
</tr>
<tr>
<td>80</td>
<td>Special Issue of Discrete Applied Mathematics: “General Theory of Information Transfer and Combinatorics” List D</td>
<td></td>
<td>1106</td>
</tr>
<tr>
<td>81</td>
<td>Bibliography of Publications by Rudolf Ahlswede</td>
<td>Rudolf Ahlswede</td>
<td>1109</td>
</tr>
</tbody>
</table>

**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/ahlswede/zif](http://www.math.uni-bielefeld.de/ahlswede/zif)