Entwurf eines Abschlussberichtes

1 Allgemeine Angaben

Abschlussbericht für das Forschungsprojekt "Informationstheorie und Kombinatorik"

1.1 Geschäftszeichen bei der DFG

AH46/1-1, AH46/1-2, AH46/4-1

1.2 Antragsteller

Vorname, Name, akad. Grad: Rudolf Ahlswede, Dr.rer.nat., Dr.h.c.
Dienststellung: Universitätsprofessor, C-4, emeritiert seit 1.10.03
Geburtsdatum: 15.9.38, Nationalität: deutsch
E-mail–Adresse: ahlswede@math.uni-bielefeld.de
Privatadresse mit Telefon: Stapenhorststr. 150, 33615 Bielefeld, Tel. 0521/104032

1.3 Institut

Fachbereich: Fakultät für Mathematik der Universität Bielefeld
Dienstadresse: Universität Bielefeld, Postfach 100131, 33501 Bielefeld
Telefon: 0521/106–4789
Telefax: 0521/106–4743

1.4 Thema

Allgemeine Theorie des Informationstransfers und Kombinatorik

1.5 Förderungs- und Berichtzeitraum

Erstantrag 15.2.2001 - 31.8.2006, Fortsetzungsantrag 1.9.2006 - 29.2.2008

1.6 Liste der Publikationen aus diesem Projekt

Erstantrag

A. Allgemeine Theorie des Informationstransfers / General theory of information transfer

[P1] R. Ahlswede, General theory of information transfer:updated, General Theory of Information Transfer and Combinatorics, Special Issue of Discrete Applied Mathematics, to appear.

A.1 Klassische Kanäle und Quellen / Classical channels and sources

[P2] R. Ahlswede, Identification entropy, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 595-613, 2006.

[P3] R. Ahlswede and N. Cai, An interpretation of identification entropy, IEEE Trans. Inf. Theory, Vol. 52, No. 9, 4198-4207, 2006.

[P4] R. Ahlswede and N. Cai, Watermarking identification codes with related topics in common randomness, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 107-153, 2006.

[P5] R. Ahlswede, N. Cai, and Z. Zhang, Secrecy systems for identification via channels with additive-like instantaneous block encipherers, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 285-292, 2006.

[P6] R. Ahlswede and N. Cai, Transmission, identification and common randomness capacities for wire-tape channels with secure feedback from the decoder, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 258-275, 2006.

[P7] R. Ahlswede and N. Cai, Codes with the identifiable parent property and the multiple–access channel, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 249-257, 2006.

[P8] Christian Heup, L-identification for sources, Doktorarbeit, Universität Bielefeld, 2006.

[P9] R. Ahlswede, H. Aydinian, and L.H. Khachatrian Unidirectional error control codes and related combinatorial problems, in Proceedings of Eighths International Workshop on Algebraic and Combinatorial Coding Theory, 8–14 September, Tsarskoe Selo, Russia, 6–9, 2002.

[P10] R. Ahlswede, H. Aydinian, L.H. Khachatrian, and L.M. Tolhuizen, On q–ary codes correcting all unidirectional errors of a limited magnitude, to appear in the special issue dedicated to the memory of Varshamov, Abstract included in Proceedings of the International workshop on Algebraic and Combinatorial Coding Theory (ACCT), held in Kranevo, Bulgaria, June 19 – 25, 2004.

[P11] R. Ahlswede, B. Balkenhol, C. Deppe, H. Mashurian, and T. Partner, T–Shift synchronization codes, General Theory of Information Transfer and Combinatorics, Special Issue of Discrete Applied Mathematics, to appear.

A.2 Vorhersagetheorie / Prediction theory

[P12] L. Bäumer, Identification and prediction, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 2006.

A.3 Quantentheoretische Kanäle und Quellen / Quantum theoretical channels and sources

[P13] R. Freivalds and A. Winter, Quantum finite state transducers, Proc. SOFSEM 2001, Theory and Practice of Informatics, Springer, 233–242, 2001.

[P14] H. Barnum, P. Hayden, R. Jozsa, and A. Winter, On the reversible extraction of classical information from a quantum source, Roy. Soc. Lond. Proc. A Math. Phys. Eng. Sci., vol. 457, no. 2012, 2019–2039, 2001.

[P15] A. Winter, On the fidelity of two pure states, J. Phys. A, vol. 34, no. 35, 7095–7101, 2001.

[P16] P. Hayden, R. Jozsa, and A. Winter, Trading quantum for classical resourses in quantum data compression, e-print: `quant-ph/0204038`, 2002.

[P17] R. Ahlswede and N. Cai, On lossless quantum data compression and quantum variable–length codes, Chapter 6 in "Quantum Information Processing", Gerd Leuchs, Thomas Beth (Eds.), Wiley–VCH Verlag, Weinheim, Germany, 66–78, 2003.

[P18] R. Ahlswede and N. Cai, On lossless quantum data compression with a classical helper, IEEE Trans. Inf. Theory, Vol. 50, No. 6, 2004.

[P19] R. Ahlswede and V. Blinovsky, Large deviations in quantum information theory, Probl. of Inf. Transm., Vol. 39, No. 4, 373–379, 2003.

[P20] R. Ahlswede and N. Cai, A strong converse theorem for quantum multiple access channels, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 460-485, 2006.

[P21] R. Ahlswede and V. Blinovsky, Classical capacity of classical-quantum arbitrarily varying channels, IEEE Trans. Inf. Theory, Vol. 53, No. 2, 526-533, 2007.

A.4 Quantenkryptologie / Quantum cryptology

[P22] N. Cai, A. Winter, and R. W. Yeung, Quantum privacy and quantum wiretap channel, Probl. Inf. Transm., Vol. 40, No. 4, 318–336, 2004.

[P23] R. Wilmink, Quantum Broadcast Channels and New Directions in Quantum Cryptography, Dissertation, Bielefeld, 2002.
download at: `www.mathematik.uni-bielefeld.de/rwilmink/`

B. Kombinatorik

[P24] R. Ahlswede, Advances on extremal problems in number theory and combinatorics, European Congress of Mathematics, Barcelona 2000, Vol. I, 147–175, Carles Casacuberta, Rosa Maria Miró–Roig, Joan Verdera, Sebastiá Xambó–Descamps, edit., Progress in Mathematics, Vol. 201, Birkhäuser Verlag, Basel–Boston–Berlin, 2001.

B.1 Entwicklung von Methoden: Ungleichungen und Extremalprobleme / Development of methods: inequalities and extremal problems

[P25] R. Ahlswede, H. Aydinian, and L.H. Khachatrian, On shadows of intersecting families, Combinatorica 24 (4), 555–566, 2004.

[P26] R. Ahlswede and L.H. Khachatrian, Katona's intersection theorem: four proofs, Combinatorica 25 (1), 105-110, 2005.

[P27] R. Ahlswede and H. Aydinian, Sparse asymmetric connectors in communication networks, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 1056-1062, 2006.

[P28] R. Ahlswede and H. Aydinian, Construction of asymmetric connectors of depth two, submitted to a special issue of J. Combinatorial Theory, Series A, in memory of Jacobus H. van Lint, Vol. 113, No. 8, 1614-1620, 2006.

[P29] R. Ahlswede and V. Blinovsky, On switching for hypergraphs, submitted to European J. of Combinatorics.

[P30] R. Ahlswede and V. Blinovsky, About the number of step functions with restrictions, Probability Theory and Applications, Vol. 50, No. 4, 537-560, 2006.

[P31] R. Ahlswede and V. Blinovsky, Multiple packing in sum-type metric spaces, General Theory of Information Transfer and Combinatorics, Special Issue of Discrete Applied Mathematics, to appear.

[P32] R. Ahlswede and V. Blinovsky, Correlation inequalities in function spaces, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 572-577, 2006.

[P33] R. Ahlswede, Another diametric theorem in Hamming spaces: optimal group anticodes, Proceedings of the IEEE Information Theory Workshop, March 13-17 in Punta del Este, 2006.

B.2 Extremalprobleme unter Dimensionsbeschränkungen/ Extremal problems under dimensions constraints

[P34] R. Ahlswede, H. Aydinian, and L.H. Khachatrian, Maximal antichains under dimension constraints, Discrete Mathematics, Special issue: EuroComb'01 – Edited by J. Nesetril, M. Noy and O. Serra, Vol. 273, No. 1–3, 23–29, 2003.

[P35] R. Ahlswede, H. Aydinian, and L.H. Khachatrian, Forbidden (0,1)–vectors in hyperplanes of $\mathbb{R}^n$: the restricted case, Designs, Codes and Cryptography, 29, 17–28, 2003.

[P36] R. Ahlswede, H. Aydinian, and L.H. Khachatrian, Forbidden (0,1)–vectors in hyperplanes of $\mathbb{R}^n$: the unrestricted case, Designs, Codes and Cryptography 37, 151-167, 2005.

[P37] R. Ahlswede, H. Aydinian, and L.H. Khachatrian, On Bohman's conjecture related to a sum packing problem of Erdös, Proceedings of the American Mathematical Society, Vol. 132, No. 5, 1257–1265, 2004.

[P38] R. Ahlswede, H. Aydinian, and L.H. Khachatrian, Intersection theorems under dimension constrains, J. Combin. Theory Ser. A, 113, 483-519, 2006.

B.3 Kombinatorische Zahlentheorie / Combinatorial Number Theory

[P39] R. Ahlswede, L.H. Khachatrian, C. Mauduit, and A. Sárközy, A complexity measure for families of binary sequences Periodica Mathematica Hungarica, Vol. 46 (2), 107–118, 2003.

[P40] R. Ahlswede, C. Mauduit, and A. Sárközy, Large families of pseudorandom sequences of k symbols and their complexity, Part I, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 293-307, 2006.

[P41] R. Ahlswede, C. Mauduit, and A. Sárközy, Large families of pseudorandom sequences of k symbols and their complexity, Part II, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 308-325, 2006.

[P42] R. Ahlswede, J. Cassaigne, and A. Sárközy, On the correlation of binary sequences, General Theory of Information Transfer and Combinatorics, Special Issue of Discrete Applied Mathematics, to appear.

[P43] R. Ahlswede and V. Blinovsky, Maximal sets of integers not containing $k+1$ pairwise coprimes and having divisors from a specified set of primes, Special Issue in Honor of Jacobus H. van Lint of J. Combinatorial Theory, Series A, Vol. 113, No. 8, 1621-1628, 2006.

[P44] R. Ahlswede and V. Blinovsky, Maximal sets of ideals without coprimes, submitted to J. Number Theory.

[P45] R. Ahlswede, The final form of Tao's inequality relating conditional expectation and conditional mutual information, Advances in Mathematics of Communications, Vol. 1, No. 2, 239-242, 2007.

B.4 Sortieren und Suchen / Search and sorting

[P46] R. Ahlswede and N. Cai, A Kraft–type inequality for d–delay binary search codes, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 704-706, 2006.

[P47] R. Ahlswede and N. Cai, Search with noisy and delayed responses, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 695-703, 2006.

[P48] R. Ahlswede, B. Balkenhol, C. Deppe, and M. Fröhlich, A fast suffix–sorting algorithm, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 719-734, 2006.

[P49] R. Ahlswede, Rate–wise optimal non–sequential search strategies under a cardinality constraint on the tests, General Theory of Information Transfer and Combinatorics, Special Issue of Discrete Applied Mathematics, to appear.

[P50] F. Cicalese and C. Deppe, Perfect ,minimally adaptive q-ary search with unreliable tests, Journal of Statistical Planning and Inference, Vol. 137, No. 1, 162-175, 2006.

[P51] F. Cicalese and C. Deppe, Quasi-perfect minimally adaptive q-ary search with unreliable tests, Algorithms and Computation, Lecture Notes in Computer Science, Vol. 2906, Springer Verlag, 527 - 536, 2003.

[P52] F. Cicalese and C. Deppe, q-ary Ulam-Renyi game with constrained lies, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 678-694, 2006.

[P53] F. Cicalese, C. Deppe, and D. Mundici, q-ary Ulam-Renyi game with weighted constrained lies, Proceedings of 10th Annual International Conference on Computing and Combinatorics- COCOON'2004, Lecture Notes in Computer Science, Vol. 3106, 82-91, 2004.

[P54] R. Ahlswede, F. Cicalese, and C. Deppe, Searching with lies under error transition cost constraints, General Theory of Information Transfer and Combinatorics, Special Issue of Discrete Applied Mathematics, to appear.

[P55] C. Deppe, Strategies for the fixed Renyi-Ulam Game with fixed number of lies, Theoretical Computer Science 314, 45-55, 2004.

[P56] C. Deppe, A survey of new results in coding with feedback and searching with lies, Information and Communication Security, Series D, IOS Press, to appear.

[P57] C. Deppe and H. Schnettler, On the $\frac{3}{4}$ - conjecture for fix-free codes, Discrete Mathematics and Theoretical Computer Science, Seminar Proceedings, Volume AE, 111-116, 2005.

[P58] R. Ahlswede, C. Deppe, and V. Lebedev Nonbinary error correcting codes with noiseless feedback, localized errors or both, Annals of European Academy of Science, No. 1, 285 - 309, 2005.

C. New Directions

C.1 Statistics and Identification

[P59] R. Ahlswede and E. Haroutunian, On logarithmically asymptotically optimal testing of hypothesis and identification, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 553-571, 2006.

[P60] R. Ahlswede, E. Haroutunian, and E. Aloyan, On logarithmically asymptotically optimal hypothesis testing for arbitrarily varying source with side information, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 547-552, 2006.

C.2 Information and Evolution

[P61] R. Ahlswede, E. Arikan, L. Bäumer, and C. Deppe, Information theoretic models in language evolution, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 769-787, 2006. Accepted as extended abstract Language Evolution and Information Theory in ISIT, Chicago June 27-July 2, 2004.

C.3 Network Coding

[P62] R. Ahlswede and S. Riis, Problems in Network coding and error correcting codes, NETCOD 2005 (The First Workshop on **Network Coding Theory** and Applications), Trento Italy, April 7, 2005, see also General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 861-897, 2006.

Fortsetzungsantrag

B.1 Entwicklung von Methoden: Ungleichungen und Extremalprobleme / Development of methods: inequalities and extremal problems

[P63] R. Ahlswede and F. Soloveva, Further diametric theorems in Lee- and other spaces, in preparation.

B.4 Sortieren und Suchen / Search and sorting

[P64] R. Ahlswede, F. Cicalese, C. Deppe, and U. Vaccaro, Two batch search with weighted lies, IEEE Trans. Inf. Theory, submitted.

C.4 Security in Database

[P65] R. Ahlswede and H. Aydinian, On security of statistical databases, SIAM Journal on Discrete Mathematics, submitted.

2 Arbeits- und Ergebnisbericht

2.1 Ausgangsfragen und Zielsetzung des Projektes

Folgende Gebiete wurden vorrangig als Forschungsfelder im Erstantrag vorgesehen

A. Allgemeine Theorie des Informationstransfers

- A.1 Klassische Kanäle und Quellen
- A.2 Vorhersagetheorie
- A.3 Quantentheoretische Kanäle und Quellen
- A.4 Quantenkryptologie

B. Kombinatorik

- B.1 Entwicklung von Methoden: Ungleichungen und Extremalprobleme
- B.2 Extremalprobleme unter geometrischen Schranken
- B.3 Kombinatorische Zahlentheorie
- B.4 Sortieren und Suchen

Folgende Gebiete wurden während der ersten Phase neu in das Projekt mit aufgenommen:

C. New Directions

C.1 Statistics and Identification

C.2 Information and Evolution

C.3 Network Coding

2.2 Darstellung der erreichten Ergebnisse

Erstantrag

Apart from the funding granted by the DFG the project also received financial strengthening by the much more broadly applied 3 year research project "General Theory of Information Transfer and Combinatorics", led by us, at the Zentrum für interdisziplinäre Forschung (ZiF) with the intensive research year 1.10.02-31.8.03. Within this scope it was in particular possible to relieve the DFG project financially, so that its period of time extended itself by about 2 1/2 years.
The interaction with about 100 fellows in two weekly seminars of four hours each led to fundamental ideas and publications, which for a large part, but not exclusively, appeared in the book "General Theory of Information Transfer and Combinatorics", Lecture Notes in Computer Science, Springer Verlag, Vol. 4123, 2006 and appear in a Special Issue of Discrete Applied Mathematics.
While discussing contributions to the areas A.1-A.4 and B.1-B.4 we indicate also connections to the questions (1)-(42), which are formulated in the original project (Erstantrag).

A.1

We start with one of the key results. Transmission, identification and common randomness, via a wiretap channel with secure feedback are studied in the work [P6]. Recall that wiretap channels were introduced by A. D. Wyner [28] and were generalized by I. Csiszár and J. Körner [15]. Its identification capacity was determined by R. Ahlswede and Z. Zhang in [9]. In the article here secure feedback is introduced to wiretap channels. Here by secure feedback we mean that the feedback is noiseless and that the wiretaper has no knowledge about the content of the feedback except via his own output. Lower and upper bounds to the transmission capacity are derived. The two bounds are shown to coincide for two families of degraded wiretap channels,

including Wyner's original version of the wiretap channel. The identification and common randomness capacities for the channels are completely determined. Also **here again identification capacity is much bigger than common randomness capacity**, because the common randomness used for the (secured) identification needs not to be secured! (ad (1))

In the work of Z. Zhang [29] the scheme of encrypting the data X^n by using the key set K^n and function $f : K^n \times X^n \to Y^n$ is considered. Under given distribution of X^n the value of the conditional entropy $\frac{1}{n}H(K^n|Y^n)$ which is offered as the measure of the secrecy of the system is investigated. In several natural cases an expression for this measure (which is called 'key equivocation rate') in terms of sizes of alphabets and distributions of X^n is derived. The secrecy system with ALIB encipherers was investigated in [6] and is adapted in [P5] to satisfy the model of identification via channels. The smallest key rate of the ALIB encipherers needed for the requirement of security is analyzed. (ad (1))
In [P4] we discuss the watermarking identification introduced by Y. Steinberg and N. Merhav. It is assumed in their model that the attacker uses a single channel known by both, information hider and decoder, and the decoder either completely knows the covertext or knows nothing about it. Thus Steinberg and Merhav asked for more robust watermarking systems i.e., the attacker can choose an unknown attack channel from a family of channels, and more general watermarking models i.e., the decoder has side information about the covertext. To answer their questions we present a direct coding theorem of identification watermarking codes for compound channels with the presence of side information at the decoder. To construct the codes we establish coding theorems for the related common randomness.(ad(1))
Shannon (1948) has shown that a source $(\mathcal{U}, P, U)$ with output U satisfying Prob $(U = u) = P_u$, can be encoded in a prefix code $\mathcal{C} = \{c_u : u \in \mathcal{U}\} \subset \{0, q-1\}^*$ such that for the entropy

$$H(P) = \sum_{u\in\mathcal{U}} -p_u \log p_u \leq \sum p_u ||c_u|| \leq H(P) + 1,$$

where $||c_u||$ is the length of c_u. In [P2] a prefix code $\mathcal{C}$ is used for another purpose, namely noiseless identification, that is every user who wants to know whether a u ($u \in \mathcal{U}$) of his interest is the actual source output or not can consider the RV C with $C = c_u = (c_{u_1}, \dots, c_{u||c_u||})$ and check whether $C = (C_1, C_2, \dots)$ coincides with c_u in the first, second etc. letter and stop when the first different letter occurs or when $C = c_u$. Let $L_{\mathcal{C}}(P, u)$ be the expected number of checkings, if code $\mathcal{C}$ is used. Discovered is an identification

entropy, namely the function

$$H_{I,q}(P) = \frac{q}{q-1}\left(1 - \sum_{u\in\mathcal{U}} P_u^2\right).$$

We prove that $L_{\mathcal{C}}(P,P) = \sum\limits_{u\in\mathcal{U}} P_u\ L_{\mathcal{C}}(P,u) \geq H_{I,q}(P)$ and thus also that

$$L(P) = \min_{\mathcal{C}} \max_{u\in\mathcal{U}} L_{\mathcal{C}}(P,u) \geq H_{I,q}(P)$$

and related upper bounds, which demonstrate the operational significance of identification entropy in noiseless **source coding similar as Boltzmann/Shannon entropy does in noiseless data compression.** It has been brought to our attention that in Statistical Physics an entropy $S_\alpha(P) = f(\alpha)(1 - \sum_{u\in\mathcal{U}} P_u^\alpha)$ has been used in Equilibrium Theory for more pathological cases, where Boltzmann's $H(P)$ fails. Attempts to find operational justifications in Coding Theory have failed. It is important here that $S_\alpha(P)$ (in particular also $S_2(P)$), which is to be compared with $H_{I,q}(P)$, does not have the parameter q, the size of the alphabet for coding. The factor $\frac{q}{q-1}$ equals the sum of the geometric series $1 + \frac{1}{q} + \frac{1}{q^2} + \ldots$, which also has an operational meaning for identification as explained in [P3]. $H(P)$ also has a q in its formula, it is the basis of the log- function for which Shannon's result holds! We emphasize, that storing the outcome of a source as a leaf in a prefix code **constitutes a data structure which is very practical.** Let for instance the c_u specify the person u out of a group $\mathcal{U}$ of persons, who has to do a certain service. Then every person traces along the tree to find out whether he/she has to go on service. We know that its expected reading time is always < 3 no matter how big $|\mathcal{U}|$ is. This goes so fast, because the persons care in this model only about themselves. If they don't have service, then they don't care in this model who has. Finding out the latter takes time $\sim H(P)$ and goes to infinity as $H(P)$ does. Notice that $H_{I,q} \leq \frac{q}{q-1} \leq 2$.
Recently we learned that J. Havrda and F. Charvát ([21]) introduced already in 1967 an entropy, which for $\alpha = 2$ coincides with identification entropy for $q = 2$. There are no applications and cases $q > 2$ are not covered. (ad (3))
C. Heup introduced in his dissertation [P8] a related L-identification entropy. (ad (4) and (5)).
Codes with identifiable parent property were introduced by H.D.L. Hollmann, J.H. van Lint, J.P. Lennartz, and L.M.G.M. Tolhuizen [22] for protection of copyright. Let a^n and b^n be two words of the same length from a finite alphabet. Then a descendant of them is a word of the same length such that each component coincides with the corresponding component of either a^n or

b^n, who are called its parents. Identifiable parent property of a code means that one can discover at least one parent from the descendant of any pair of codewords in the code. R. Ahlswede and N. Cai observed in [P7] its relation with coding for multiple access channels. Its probabilistic version is coding for a multiple access channel such that two senders have the same codebook and the receiver has to decode the message at least from one of the two senders. This leads them to a coding problem for the multiple access channel, where the two senders are allowed to use different codebooks and again the receiver only needs to decode the message sent by anyone of the two senders. The capacity region is determined and the result shows that an optimal strategy for the receiver is to always decode the message from a fixed sender. The result has a simple consequence for the interference channel with one deterministic component which seems to be new.
In [P9] and [P10] we studied a special type of q-ary unidirectional and asymmetric error correcting codes. In these codes the number of errors can be very big, however the magnitude of error (referred to as level) is bounded. These codes are of practical use in many real communication systems. A class of optimal q-ary codes correcting all unidirectional errors of a given level has been constructed.
The model considered in [P11] has applications when storing information on digital media. The corresponding T-shift synchronization codes of a fixed block length generalize the cover free codes. We construct a family of T-shift synchronization codes, which are asymptotically optimal for an infinite number of values of T.

A.2

The results of L. Bäumer's phd thesis were published in [P12].

A.3 and A.4

This work received financial support in part also from DFG-AH 46/2. We refer to our final report (Abschlussbericht) there. We just point out here two highlights, [P20] and [P21], relating to the fundamental question of finding **quantum versions of classical methods.**
The first paper [P20] is on classical quantum multiple access channels. The coding and weak converse theorem for classical multiple access channels of [1] was extended to classical quantum multiple access channels in [27]. But the extension of the strong converse theorem has been open for several years. One reason, but likely not the only one, for it is that so far an analogue to the Blowing Up Lemma [7] has not been discovered. Also other methods failed. However the **Wringing Technique**, a powerful technique of [4], could be extended In [P20] to the quantum case and then gave the desired strong converse. We expect that the work not only helps us to better **understand quantum multiple access channels**, but also brings new ideas and tech-

niques into the whole area of quantum multi-user information theory.
We conclude now with the second paper [P21]. We prove that the average error capacity C_q of a quantum arbitrarily varying channel (QAVC) equals 0 or else the random code capacity $\bar{C}$ (Ahlswede's dichotomy). We also establish a necessary and sufficient condition for $C_q > 0$. It is interesting to note, that in our proof of Theorem 1 we essentially use the elimination technique (an early candidate of what is now called derandomization in Computer Sciences) from [2], which gives Lemma 2. This is the analogue of the main result of [2]. There a necessary and sufficient condition for positivity of the capacity was given, if the set of transmission matrices is row-convex closed– that is under a practically satisfactory assumption of robustness. The mathematical problem of characterizing positivity without this assumption in terms of symmetrizability was started in [18] and completely solved in [16] with a non-standard decoding rule and without use of the elimination technique of [2]. (Using this technique and proving directly that non-symmetrizability implies positive capacity is a basic problem, which is open for more than 20 years!) On the other hand in the present quantum case we have not found a suitable decoding rule and follow the elimination technique (Lemma 2). Analogously the positivity problem for the QAVC can be settled by reducing it to a related classical AVC to which then the result of [16] can be applied. We emphasize that the very hard maximal error capacity problem for AVC (including Shannon's zero error capacity problem as special case) is based on a more realistic communication model. It was solved for a nice class of channels in [3], where for the first time in the area of AVC a non standard decoding rule was used. Extension to QAVC constitutes a challenging problem!

B.1

A Kruskal-Katona type theorem has been proved in [P25] for intersecting families. Namely, let $\mathcal{A}$ be a t-intersecting family of k-sets over the set of positive integers. For given k, t and l we give an exact lower bound for the l-shadow of $\mathcal{A}$, if $\mathcal{A}$ is big enough. Moreover, we give the configuration of an optimal family, which turns to be one of "Frankl's families". (ad (19))
[P26] contains the simplest proof for Katona's Intersection Theorem. (ad (19))
A communication network is modelled as an acyclic directed graph $G = (V, E)$ with some distinguished vertices called inputs and other distinguished vertices called outputs. The remaining vertices are called links. There are two parameters of particular interest in comparing networks: the size and the depth. The size (the number of edges) in some approximate sense corresponds to the cost of the network. The depth (the length of the longest path from an input to an output of the network) corresponds to the

delay of the transmission in the network. Therefore in designing communication networks it is desirable to achieve smaller size and smaller depth. An (n, N, d)-connector or rearrangeable network is a network with n inputs, N outputs and depth d, in which for any injective mapping of input vertices into output vertices there exist n vertex–disjoint paths joining each input to its corresponding output. The problem of designing optimal connectors goes back to works of Shannon, Slepian et al. ([24], [25], [14], [10]) started in the 50's. In [P26] asymmetric connectors (connectors with $n \ll N$) of depth two are considered. A simple combinatorial construction of sparse connectors is given, which is based on the Kruskal/Katona Theorem for shadows of families of k-element subsets. Fault–tolerance of the constructed connectors is also considered. Further improvements were obtained in [P28] by using other theorems for shadows. The results are in general and also in most special cases the presently best.

We found the asymptotics of the number of labelled uniform hypergraphs with given degree sequences in [P29] by using a new switching algorithm. [P30] gives progress on Young Tableaux and [P31] generalizes work of V. Blinovsky from Hamming to general sum-type metric spaces. The rate-wise optimal results find applications to search with lies with general cost constraints introduced in [P57].

B.2

Problem: At most how many (0,1)-vectors of given weight can be embedded in a k-dimensional subspace of $\mathbb{R}^n$?

Solving in [P34] this long standing geometrical extremal problem first raised by Longstaff (1977) and by Odlyzko (1981) was the starting point for developing a new area : Extremal Problems under Dimension Constraints. Some recent results, conjectures and research problems can be found in [P35], [P36] and forthcoming work in J. Comb. Theory on Intersecting systems under dimension constraints. (ad (22))

An extremal problem raised by Bohman in connection to a sum packing problem of Erdös was studied in [P37]. In particular, we disproved Bohman's conjecture stating a new conjecture for this problem. (ad (26))

A very basic inequality, known as the Ahlswede-Daykin inequality and called Four Function Theorem by some authors, which is more general and also sharper than known correlation inequalities in Statistical Physics, Probability Theory, Combinatorics and Number Theory (see the preface and survey by Fishburn and Shepp [19]) is extended elegantly to function spaces in [P32]. That is, the inequality of the same type holds for a Borel measure on $R^{[0,1]}$. We expect that it will have wide applications.

It seems that with [P33] a new direction started. In the last century together with Levon Khachatrian we established a diametric theorem in Hamming

space $\mathcal{H}^n = (\mathcal{X}^n, d_H)$. Now we contribute a diametric theorem for such spaces, if they are endowed with the group structure $\mathcal{G}^n = \sum_1^n \mathcal{G}$, the direct sum of group $\mathcal{G}$ on $\mathcal{X} = \{0, 1, \ldots, q-1\}$, and as candidates are considered which form a **subgroup** of $\mathcal{G}^n$. For all finite groups $\mathcal{G}$, every permitted distance d, and all $n \geq d$ subgroups of $\mathcal{G}^n$ with diameter d have maximal cardinality q^d. **Other extremal problems can also be studied in this setting**.

B.3

It was planned to continue with A. Sárközy our investigations of extremal sets of numbers, especially primitive sets. Unfortunately, various obligations prohibited to work on the problems (33)-(44), but we still want to do it! On the other hand, occasional meetings in Luminy and in Bielefeld, also with C. Mauduit and J. Cassaigne, led to nice number theoretical contributions to Cryptology.

The papers are devoted to the investigation of the problem of generating pseudorandom sequences and their statistical properties. This is an important task for cryptology since for instance these pseudorandom sequences can serve as a source of key bits needed for encryption. The first problem in [P40] is to find a proper test for sequences of elements from a finite alphabet to be pseudorandom. For a binary sequence with alphabet $\{-1, +1\}$ the authors choose the criterium of a small modul of the sum of subsets of the elements of the sequence maximized over the choice of the subset of positions of these elements and small correlation measure which is the absolute value of the sum of products of elements from some set of subsets of positions maximized over the special choice of the positions of these elements. Then these measures are extended in [P41] to a nonbinary alphabet and as one generalization the frequency criterium is chosen, i.e. the deviation of the number of given patterns on given positions from the expected value, maximized over the choice of the positions. Relations are proved which show the equivalence (in some sense) of these different tests of pseudorandomness in the binary case. Also proved is that the number of the sequences with large measures of pseudorandomness is exponentially small in comparison with the number of all sequences. Algorithms were introduced in for constructing pseudorandom sequences. These constructions can find applications in cryptology and simulations. Also considered were the notion of $f-$complexity of the set of $n-$tuples which is the maximal number t s.t. arbitrary t positions have an arbitrary pattern in some $n-$tuple from this set, which was introduced in [P39] and correlation properties of binary sequences ([P42]).

More explanations are given by the excellent introductions also in earlier work, where C. Mauduit and A. S'arközy explain their approach to cryptology. Roughly speaking their philosophy is that less can be more: instead of going

after complex problems whose high complexity till now cannot be proved and therefore always there can be a bad end of a dream, they suggest to work with number theoretical functions of likely not highest complexity, but for which some degree of complexity can be proved.
Together with V. Blinovsky classical number theoretical extremal theory was advanced in [P43].
A decade ago Ahlswede and Khachatrian settled a problem of Erdös about maximal sets of positive integers less than n not containing $k+1$ pairwise coprimes and also a problem of Erdös and Graham concerning the maximal value of k with integers $1 < a_1 < \cdots < a_k = n$, $(a_i, a_j) \neq 1$. Actually this problem was solved in a more general and seemingly more natural setting reflected in the phrase "having divisors from a specified set of primes". All this work, related work and the history of the problems is reported in the survey [P24]. *The present work is indicated in our title, which refers to a common generalization of both these problems and their corresponding theorems.*
These authors also found an extension to algebraic number fields [P43]. There they prove that for all sufficiently large N_0 the maximal set of ideals of the maximal order of the algebraic number field, such that any pair of ideals from this set is not coprime and norm of each ideal does not exceed N_0 is the set $E(N_0) = \{\theta : N(\theta) \leq N_0,\ \theta = \eta_1 u\}$, where $\{\eta_1, \eta_2, \ldots\}$is the set of prime ideals of the maximal order and $N(\eta_3) > 2$.
The famous Green/Tao result says that the primes have arbitrary long arithmetical progressions. Subsequently Tao found a novel connection:
Information Theory as tool for Graph Theory and Number Theory The final form of Tao's inequality relating conditional expectation and conditional mutual information
Recently Terence Tao ([26]) approached Szemerédi's Regularity Lemma from the perspectives of Probability Theory and of Information Theory instead of Graph Theory and found a stronger variant of this lemma, which involves a new parameter.
To pass from an entropy formulation to an expectation formulation he found the following
Lemma. Let Y, and X, X' be discrete random variables taking values in $\mathcal{Y}$ and $\mathcal{X}$, respectively, where $\mathcal{Y} \subset [-1, 1]$, and with $X' = f(X)$ for a (deterministic) function f.
Then we have

$$\mathbb{E}\big(|\mathbb{E}(Y|X') - \mathbb{E}(Y|X)|\big) \leq 2I(X \wedge Y|X')^{\frac{1}{2}}.$$

We show that the constant 2 can be improved to $(2\ell n 2)^{\frac{1}{2}}$ and that this is the best possible constant.

B.4

Enrichments for the project are gained from relations between coding for channels with feedback and search problems (c.f. [8]).
For example error-correcting codes with feedback, which were introduced by Berlekamp [11] are equivalent to the following search problem. A search space $\mathcal{M} = \{1, \ldots, M\}$ is given and we want to find one (say defective) element. In every step we perform a test by choosing a subset of $\mathcal{M}$. When working correctly the test produce a "Yes", if the defective element is in the subset and otherwise it produces a "No". The main problem is that the tests not always give the correct answer. In our model we assume that the number of incorrect answers is restricted.
This search model is often described equivalently as "Renyi-Berlekamp-Ulam-Game". The models readily extends to q alternatives for answers $Q = \{0, 1, \ldots, q-1\}$. **The new idea, which was developed in [P49], is to consider error cost constraints.** That means, there is a function $\Gamma : \mathcal{Q} \times \mathcal{Q} \to \mathbb{N}$. The function Γ is meant to weigh the answers. Whenever an answers t to a question (a test), whose answer is s, is given the answer has weight $\Gamma(t, s)$. It is allowed to give false answers with total weight up to e.
In [P52] the authors assume some symmetry of Γ and weights 0 and 1. They provide a lower bound on the number of questions needed to solve the problem and prove that in infinitely many cases this bound is attained by (optimal) search strategies. Moreover they prove that, in the remaining cases, at most one question more than the lower bound is always sufficient to successfully find the unknown element. All strategies also enjoy the property that among all possible adaptive strategies they use the minimum amount of adaptiveness during the search process. In [P54] the general weighted case is considered. We give an asymptotically exact solution if the positive minimal weight w of Γ is a divisor of e.

A coding scheme for delayed feedback, which shows that in this case the capacities of all memoryless channels with non-delayed feedback can be achieved, is given in [P47]. A characterization of the zero-error capacity of a DMC and the average-error capacity of an AVC, when the delay time increases linearly with the length of the codes, is also obtained.

In [P46] the Kraft inequality for d-DBS codes is sharpened, based on the work of Ambains-Bloch-Schweizer, who introduced these codes.
A new suffix sorting algorithm to sort all suffixes of a string $x^n \in \{0, \ldots, k-1\}^n$ lexicographically is developed in [P48]. It computes the suffix sorting in $O(n)$ space and $O(n^2)$ time in the worst case. It has also the property that it sorts the suffixes lexicographically correctly according to the prefixes of

length $\log_k \lceil \frac{n}{2} \rceil$ in the worst case in linear time.
Already in his Lectures on Search Renyi suggested to consider a search problem, where an unknown $x \in \mathcal{X} = \{1, 2, \ldots, n\}$ is to be found by asking for containment in a minimal number $m(n,k)$ of subsets $A_1, \ldots, A_m$ with the restrictions $|A_i| \leq k < \frac{n}{2}$ for $i = 1, 2, \ldots, m$.
Katona gave in 1966 the lower bound $m(n,k) \geq \frac{\log n}{h\left(\frac{k}{n}\right)}$ in terms of binary entropy and the upper bound $m(n,k) \leq \left\lceil \frac{\log n+1}{\log n/k} \right\rceil \cdot \frac{n}{k}$, which was improved by Wegener in 1979 to $m(n,k) \leq \left\lceil \frac{\log n}{\log n/k} \right\rceil \left(\lceil \frac{n}{k} \rceil - 1 \right)$. *We prove here for* $k = pn$ *that* $m(n,k) = \frac{\log n + o(\log n)}{h(p)}$, *that is, ratewise optimality of the entropy bound:* $\lim\limits_{n\to\infty} \frac{m(n,pn)}{\log n} = \frac{1}{h(p)}$. Actually this work was motivated by a more recent study of Karpovsky, Chakrabarty, Levitin and Avresky of a problem on fault diagnosis in hypercubes, which amounts to finding the minimal number $M(n,r)$ of Hamming balls of radius $r = \rho n$ with $\rho \leq \frac{1}{2}$ in the Hamming space $\mathcal{H}^n = \{0,1\}^n$, which separate the vertices. Their bounds on $M(n,r)$ are far from being optimal. We establish bounds implying $\lim_{n\to\infty} \frac{1}{n} \log M(n,r) = 1 - h(\rho)$. However, it must be emphasized that the methods of prove for our two upper bounds are quite different.
In [P57] we consider the question, whether there exists a fix-free code for a given sequence of codeword lengths. We introduce general π-systems, which are special kinds of fix-free codes with Kraftsum $\left\lceil \frac{q}{2} \right\rceil q^{-1}$. We show, that π-systems with only two neighbouring levels and $L \cdot \left\lceil \frac{q}{2} \right\rceil$ codewords on the first level exist, if and only if there exists a $\lceil \frac{q}{2} \rceil$-regular subgraph of the directed de Bruijn graph $\mathcal{B}_q(n)$ with n edges over a q-ary alphabet with L vertices. Furthermore we show that arbitrary one level π-systems exist. With this method the range of validity of the $\frac{3}{4}$-conjecture was significantly enlarged.
A famous problem in coding theory consists in finding good bounds for the maximal size, say $M(n,t,q)$, of a t-error correcting code over a q-ary alphabet $Q = \{0, 1, \ldots, q-1\}$ with blocklength n. Suppose now that having sent letters $x_1, \ldots, x_{j-1}$ the encoder knows the letters $y_1, \ldots, y_{j-1}$ received before he sends the next letter x_j $(j = 1, 2, \ldots, n)$. We then have the presence of a noiseless feedback channel. We investigate in [P58] the q-ary case. Again the Hamming bound for $C_q(\tau)$, the maximal rate achievable for τ and all large n, is a central concept. For the feedback model we present here a coding scheme based on an idea of deletions. It is easy to analyse and yield also Berlekamp's results for the case $q = 2$. We turn now to the model with localized errors. Suppose that the **encoder**, who wants to encode message $i \in \{1, 2, \ldots, M\}$, knows the t-element set $E \subset [n] = \{1, \ldots, n\}$ of positions, in which only errors may occur. He then can make the codeword presenting i dependent

on $E \in \mathcal{E}_t = \binom{[n]}{t}$, the family of t-element subsets of $[n]$. Whereas all this work is for block codes we next investigate variable length codes with all lengths bounded from above by n. The end of a word carries the symbol $\square$ and is thus recognizable by the decoder. Very important here is that the lengths carry **sure** data which can be used as a "protocol" information. For both, the $\square$-model with feedback and the $\square$-model with localized errors, the Hamming bound is the exact capacity curve for $\tau < 1/2$. Somewhat surprizingly, whereas with feedback the capacity curve coincides with the Hamming bound also for $1/2 \leq \tau \leq 1$, in this range for localized errors the capacity curve equals 0. Also notice that without the marker $\square$ in the range $0 \leq \tau < 1/2$ with feedback the capacity curve is **smaller** than that for localized errors. Also we give constructions in the $\square$-model with both, feedback and localized errors. Finally, in the standard model with feedback **and** localized errors the help of feedback is adressed. We give an optimal construction for one-error correcting codes with feedback and localized errors.

C.1

A broad class of statistical problems arises in the framework of hypothesis testing in the spirit of identification for different kinds of sources, with complete or partial side information or without it. [P60] is devoted to the investigation of a hypothesis testing problem for arbitrarily varying sources with complete side information. [P59] considers the more difficult but more promising problem of hypothesis identification.

C.2

In [P61] readers find an interesting application of Information Theory in the study of Language Evolution. The model was originally introduced by M.A. Nowak and D.C. Krakauer [23], where the fitness of a language is introduced. For this model they showed if signals can be mistaken for each other, then the performance of such systems is limited. The performance cannot be increased over a fixed threshold by adding more and more signals. Nevertheless the concatenation of signals or phonemes to words increases significantly the fitness of the language. The fitness of such a signalling-system depends on the number of signals and on the probabilities to transmit individual signals correctly. R. Ahlswede, E. Arikan, L. Bäumer and C. Deppe investigated optimal configurations of signals in different metric spaces. In [P61] we **prove for all metrics with a positive semidefinite associated matrix a conjecture by Nowak** including all important metrics studied by different authors in this direction. The conjecture holds for all ultra-metric spaces. Especially the authors analyze the Hamming space. In this space the direct consequence of the theorem is that the fitness of the whole space equals the maximal fitness and the fitness of Hamming codes asymptotically achieves this maximum.These theoretical models of fitness of a language enable the

investigations of traditional information theoretical problems in this context, in particular, for feedback problems, transmission problems for multi-way channels etc. It is shown that feedback increases the fitness of a language.

C.3

The paper [P62] has been discussed in 2.1.

C.4

In the recent paper [P61] it is shown that the work under B.2 finds applications in Statistical Database Security (see [20]) and settles several of the problems there.

Fortsetzungsantrag

In the short phase of the sequel proposal (31.8.2006-29.2.2008) only some tasks could be worked on with the granted resources (7 BAT IIa positions for one year were applied for and 1.5 positions for one year could be given). Progresses were achieved in B.1 (Development of Methods: Inequalities and Extremal Problems) B.4 (Search and Sorting), and C.4 (Security in Database), which are explained beneath.

B.1

Ahlswede and Soloveva considered in [P63] .....

B.4

In [P64] we close the gap between the bounds of [P54] (see first phase B.4) and provide matching upper and lower bounds also if w is not a divisor of e.

C.4

A statistical database (SDB), considered in [P65], is a database that is used to return statistical information derived from the records to user queries for statistical data analysis. Sometimes, by correlating enough statistics, confidential data (stored in a SDB) about an individual can be inferred. Examples of confidential information stored in a SDB might be salaries or data concerning the medical history of individuals. An important problem is to provide security to SDB against the disclosure of confidential information. A statistical database is said to be secure if no protected data can be inferred from the available queries. One of the security-control methods suggested in the literature consists of query restriction: the security problem is to limit the use of the SDB, introducing a control mechanism, such that no protected data can be obtained from the available queries. Chin and Ozsoyoglu [13] introduced a control mechanism, called Audit Expert, where only SUM queries, that is only certain sums of individual records, are available for the users. This SUM query model leads to several challenging optimization problems. Assume there are n numeric records $\{z_1, \ldots, z_n\}$ stored in a database. A natural problem is to maximize the number of answerable SUM queries, that

is the number of subset sums of $\{z_1, \ldots, z_n\}$ (possibly with some additional constraints) that can be returned, such that none of numbers z_i (or sums of subsets with the size not exceeding a specified number) can be inferred from these queries. In [P58] tight bounds , for the number of answerable queries, under constraints on size and dimension on inquired subsets, are obtained. We considered the problem for the g-group security model, where not only individual data but also subset sums of size g or less must be protected. Earlier only results for $g = 1$ were known. In case when the size of query sets is fixed we give exact solution to the problem and describe all optimal query sets. (The results was also presented at Dagstuhl Seminar 06201, Combin. and Algoritmic Foundations of Pattern and Association Discovery, 14 - 19, Mai, 2006). These results are heavily based on methods and tools from [5]. They improve previously known results in [12], [17] and extend them to higher dimension. In particular, a question raised by Griggs [20] is solved.
Noch nicht bearbeitete Teilgebiete für Informationsflüsse wurden im gegenwärtigen Antrag des DFG-Projektes "Informationflüsse" - wie dort unter 2.1 erläutert - mit aufgenommen.

Weitere Literaturhinweise im Ergebnisbericht

[1] R. Ahlswede, Multi-way communication channels, Proceedings of 2nd International Symposium on Information Theory, Thakadsor, Armenian SSR, Sept. 1971, Akademiai Kiado, Budapest, 23-52, 1973.

[2] R. Ahlswede, Elimination of correlation in random codes for arbitrarily varying channels, Z. Wahrscheinlichkeitstheorie und verw. Geb. 44, 159-175, 1978.

[3] R. Ahlswede, A method of coding and its application to arbitrarily varying channels, J. Combinatorics, Information and System Sciences, Vol. 5, No. 1, 10-35, 1980.

[4] R. Ahlswede, An elementary proof of the strong converse theorem for the multiple-access channel, J. Combinatorics, Information and System Sciences, Vol. 7, No. 3, 216-230, 1982.

[5] R. Ahlswede, H. Aydinian, and L.H. Khachatrian, Extremal problems under dimension constraints, Discrete Mathematics, Special issue: EuroComb'01 - J. Nesetril, M. Noy and O. Serra (Ed), Vol. 273, No. 1-3, 9-21, 2003.

[6] R. Ahlswede and G. Dueck, Bad codes are good ciphers, Probl. of Control and Inf. Theory, Vol. 11, No. 5, 337-351, 1982.

[7] R. Ahlswede, P. Gács, and J. Körner, Bounds on conditional probabilities with applications in multiuser communication, Z. Wahrscheinlichkeitstheorie und verw. Geb. 34, 157-177, 1976.

[8] R. Ahlswede and I. Wegener, Search Problems with Supplement of recent Literature, Wiley-Interscience Series in Discrete Mathematics and Optimization, 1987.

[9] R. Ahlswede and Z. Zhang, New directions in the theory of identification via channels, IEEE Trans. Inf. Theory, Vol. 41, No. 4, 1040-1050, 1995.

[10] V.E. Beneś, Optimal rearrangeable multistage connecting networks, Bell System Tech. J. 43, 1641–1656, 1964.

[11] E.R. Berlekamp, Block coding with noiseless feedback, Phd-thesis, MIT, Cambridge, MA, 1964.

[12] L. Branković, P. Horak, and M. Miller, An optimization problem in statistical databases, SIAM J. Discrete Math., Vol. 13, 346-353, 2000.

[13] F.Y. Chin and G. Ozsoyoglu, Auditing and inference control in statistical databases, IEEE Transactions on Software Engineering SE-8, 574-582, 1982.

[14] C. Clos, A study of non–blocking switching networks, Bell System Tech. J. 32, 406–424, 1953.

[15] I. Csiszár and Körner, Broadcast channel with confidential message, IEEE Trans. Inform. Theory, Vol. 24, 339-348. 1978.

[16] I. Csiszár and P. Narayan, The capacity of the arbitrarily varying channel revisited: positivity constraints, IEEE Transactions of IT, Vol. 34, No, 2, 181-193, 1988.

[17] J. Demetrovich, G.O.H. Katona, and D. Miklos, On the security of individual data, Lecture Notes in Comp. Sci., Vol. 2942, 49-58, Springer 2004.

[18] T. Ericson, Exponential error bounds for random codes in the arbitrarily varying channel, IEEE Transactions on IT, Vol. 31, No. 1, 42-48, 1985.

[19] P.C. Fishburn and L. Shepp, The Ahlswede-Daykin theorem, Numbers, Information, and Complexity, Kluwer, 501-516, 2000.

[20] J. R. Griggs, Database security and the distribution of subset sums in R^m, Graph theory and combinatorial biology (Balatonlelle, 1996), 223-252, Janos Bolyai Math. Soc., 1999.

[21] J. Havrda and F. Charvát, Quantification method of classification processes, concept of structural α-entropy, Kybernetika (Prague) 3, 30-35, 1967.

[22] H.D.L. Hollmann, J.H. van Lint, J.P. Lennartz, and L.M.G.M. Tolhuizen, On codes with the identifiable parent property, J. Combin. Theory Ser. A, Vol. 82, No. 2, 121–133, 1998.

[23] M.A. Nowak and D.C. Krakauer, The evolution of language, PNAS 96, 14, 8028-8033, 1999.

[24] C.E. Shannon, Memory requirements in a telephone exchange, Bell System Tech. J. 29, 343–349, 1950.

[25] D. Slepian, Two theorems on a particular crossbar switching network, unpublished manuscript, 1952.

[26] T. Tao, Szemeredi's regularity lemma revisited, Contrib. Discrete Math. 1, 8-28, 2006.

[27] A. Winter, The capacity region of the quantum multiple access channel, IEEE Trans. Inform. Theory, Vol. 47, No. 7, 3059–3065, 2001.

[28] A.D. Wyner, The wire-tap channel, Bell Sys. Tech. J. V. 54, 1355-1387, 1975.

[29] Z. Zhang, A simplified method for computing the key equivocation for additive-like instantaneous block encipherers, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 276-284, 2006.

2.3 Qualifikation des wissenschaftlichen Nachwuchses im Zusammenhang mit dem Projekt

- Christian Heup, The mathematical background of the advanced encryption standard, Diplomarbeit, Universität Bielefeld, 2003

- Julia Mixtacki, On two distance measures for genome comparison: the inversion and the tanslocation distance, Diplomarbeit, Universität Bielefeld, 2004
- Holger Schnettler, On the 3/4-conjecture for fix-free codes, Diplomarbeit, Universität Bielefeld, 2005
- Rainer Wilmink, Quantum broadcast channels and cryptographic applications for separable states, Doktorarbeit, Universität Bielefeld, 2003
- Christian Heup, L-identification for sources, Doktorarbeit, Universität Bielefeld, 2006.

2.4 Projektmitarbeiter

In brackets the published paper in the project.

- Lars Bäumer, wissenschaftlicher Mitarbeiter, 1.3.2001-30.6.2001

  (A.2: [P12], C.2: [P61])
- Vladimir Blinovsky, wissenschaftlicher Mitarbeiter, 1.6.2005 - 31.12.2005

  (A.3: [P19], [P21], B.1: [P29], [P30], [P31], [P32], B.3: [P43], [P44])

  Furthermore V. Blinovsky was in Bielefeld as a guest from 1.1.2007-31.3.2007 to complete together with Rudolf Ahlswede the forthcomming book " Lectures on Advances in Combinatorics". His visit was supported by this project and the "Koordinatorfond" of the DFG-Schwerpunkt SPP 1126 "Algorithmik großer und komplexer Netzwerke".
- Ning Cai, wissenschaftlicher Mitarbeiter, 2.1.2002 - 31.12.2002

  (A.1: [P3], [P4], [P5], [P6], [P7], , A.3: [P17], [P18], [P20], A.4: [P22], B.4: [P46], [P47])
- Christian Deppe, wissenschaftlicher Mitarbeiter, 1.10.2003-29.2.2008

  (A.1: [P11], B.4: [P48], [P50], [P51], [P52], [P53], [P54], [P55], [P56], [P57], [P58], [P64], C.2: [P61])
- Haik Mashurian, wissenschaftlicher Mitarbeiter, 1.10.2003 - 30.9.2004, 3.1.2005-31.3.2005

  (A.1: [P11])

3 Zusammenfassung

Im Erstantrag wurde der Erwartung Ausdruck verliehen, dass der Projektzeitraum 2001–2003 zur fruchtbarsten Periode unserer Gruppe, deren Anfänge auf dem SFB 343 "Diskrete Strukturen in der Mathematik" zurückgehen, überhaupt wird, wenn die DFG ihre gewohnte Unterstützung gibt.
Die Erwartungen in der Forschung wurden mehr als erfüllt, da das Projekt neben der von der DFG gewährten Unterstützung noch außerordentlich profitierte von dem uns gewährten Forschungsprojekt "General Theory of Information Transfer and Combinatorics" am Zentrum für interdisziplinäre Forschung (Zif) mit dem intensiven Forschungsjahr 1.10.02 – 31.8.03. In diesem Rahmen war es insbesondere möglich durch die Einstellungen von Dr. L. Bäumer in der Zeit vom 1.7.2001 – 30.9.2004 und Dr. N. Cai in der Zeit vom 1.1.2003 – 30.9.2004 als Mitarbeiter am Zif das DFG–Projekt finanziell zu entlasten. Entscheidender, die Interaktion mit etwa 100 Fellows in zwei jeweils vierstündigen wöchentlichen Seminaren während des Forschungsjahres führte zu einer Flut von Ideen und auch zahlreichen Veröffentlichungen.
In der ersten Phase des Projektes (2001-2006) gab es zwei Durchbrüche. Ein neuer Entropiebegriff, genannt Identifikationsentropie, beschreibt die mittlere Schnittzahl bei der Identifikation für Quellen angemessen (operationale Rechtfertigung des Begriffs) sowie die Boltzmann'sche Entropie die mittlere Codierlänge für Quellenspeicherungen in Shannon's Fundamentalsatz beschreibt.
Shannon's wechselseitige Information stellt sich als adäquater für die Theorie der Identifikation über störende Kanäle mit Rückkopplung heraus als dieses für die Theorie der Übertragung, für welche sie von Shannon eingeführt wurde, der Fall ist!
Daneben gab es eine ganze Reihe beachtenswerter Fortschritte. Als Beispiel sei hier hervorgehoben, dass Katona's bekannte untere Entropieschranke (siehe Ahlswede/Wegener "Suchprobleme") für trennende Systeme mit einer Kardinalitätsbeschränkung an die Teilmengen als asymptotisch optimal nachgewiesen wurde.
Eine Reihe von Ergebnissen, die gemeinsam mit Koautoren erzielt wurden, findet man in der Darstellung der erreichten Ergebnisse.
In der kurzen Phase des Fortsetzungsantrages (31.8.2006-29.2.2008) konnten mit den bewilligten Mitteln (beantragt waren 7 Jahresstellen BAT IIa und 1,5 Jahresstellen konnten gegeben werden) nur einige Aufgaben bearbeitet werden. Fortschritte wurden ermittelt zu B.4 (Search and sorting), C.1 (Statistics and Identification) und C.4 (Security in Database).