T a g u n g s b e r i c h t 8/1996

Informationstheorie: Algebraic, Combinatorial and Probabilistic Codes and Coding Techniques

18.02. bis 24.02.1996

Die Tagung fand unter der Leitung von R. Ahlswede (Bielefeld), J.H. van Lint (Eindhoven) und J.L Massey (ETH Zürich) statt.

Zusammenfassungen der Vortragenden:

Rudolf Ahlswede and Ning Cai

The arbitrarily varying channel with noiseless feedback and maximal error probability: a trichotomy of the capacity formula

Let $\mathcal{W}$ be the set of transmission matrices of the AVC with alphabets $\mathcal{X}, \mathcal{Y}$. Denote its capacity by $C_f(\mathcal{W})$. Define $\mathcal{Y}_x = \{y \in \mathcal{Y} : w(y|x) = 1 \text{ for some } w \in \mathcal{W}\}$.

We need also the sets $\overline{\mathcal{W}}$ = convex hull $(\mathcal{W})$, $\overline{\overline{\mathcal{W}}}$ = row–convex hull $(\mathcal{W})$, and $\hat{\mathcal{W}}$ = set of 0–1–matrices in $\overline{\overline{\mathcal{W}}}$.

Positivity Theorem: $C_f(\mathcal{W}) > 0 \Leftrightarrow$

(i) $C_R(\mathcal{W}) \triangleq \max\limits_{P \in \mathcal{P}(\mathcal{X})} \min\limits_{w \in \overline{\mathcal{W}}} I(P|W) > 0$ and (ii) $\mathcal{Y}_x \cap \mathcal{Y}_{x'} = \phi$ for some $x \neq x'$

Capacity Theorem (with Trichotomy)

$$C_f(\mathcal{W}) = \begin{cases} 0, & \text{if (i) or (ii) does not hold} \\ \min\big(C_R(\mathcal{W}), C_f(\hat{\mathcal{W}})\big), & \text{if } \hat{\mathcal{W}} \neq \phi \text{ and (i), (ii) hold} \\ C_R(\mathcal{W}), & \text{if } \hat{\mathcal{W}} = \phi \text{ and (i), (ii) hold} \end{cases}$$

Here $C_f(\hat{\mathcal{W}})$ was determined by the first author (1973).

Vladimir B. Balakirsky:

On interval linear complexity of binary sequences

We consider the problem of partial approximation of binary sequences by the outputs of linear feedback shift registers. A generalization of the linear complexity profiles of binary sequences leads to a sequence that is regarded as the profile of interval linear complexity. Some properties of this sequence are examined.

Marat Burnashev and Leonid Bassalygo

Authentication, identification and pairwise separated measures

We show that authentication and identification problems are equivalent to each other. Moreover, both problems are majorized (in a certain sense) by problem of pairwise separated measures. The statement of the last problem is the following.

Definition. A collection $\{\mu_i, i = 1, \ldots, M\}$ of probability measures μ_i on a finite set A is called q–separated if

$$\|\mu_i - \mu_j\| \geq 2(1 - q) \text{ for any } i \neq j.$$

Let $M(A, q)$ be the maximal possible number of q–separated prob. measures on a set $\mathcal{A}$ of card $\mathcal{A} = A$. We get a new upper bound for $M(A, q)$.

Toby Berger and Xiahai Zhang

Asymptotics of tight typicality

$X_1, \ldots, X_n$ are i.i.d.r.v. with distribution $\{p(a_i) = p_i, 1 \leq i \leq M\}$. The type, or composition, of $(X_1, \ldots, X_n)$ is the vector $\underline{K} = (K_1, \ldots, K_M)$ where $K_j = |\{i : 1 \leq i \leq n, X_i = a_j\}|$. $\underline{K}$ is multinomially distributed with components satisfying $K_1 + K_2 + \cdots + K_M = n$. A realization $\underline{k} = (k_1, \ldots, k_m)$ will be called a tightly typical type if $|k_i - np_i| < n^{\frac{1}{2}+\varepsilon}$ for $1 \leq i \leq M$, where $\varepsilon \in (0, \frac{1}{6})$ is fixed. The set $S(n, \varepsilon)$ of all tightly typical types has asymptotic probability 1 in the sense that $\lim_{n\to\infty} P(\underline{K} \in S(n, \varepsilon)) = 1$. We show the asymptotic formula

$$P(\underline{K} = \underline{k}) \sim \sqrt{2\pi n} \prod_{i=1}^{M} \frac{e^{-\frac{(k_i - np_i)^2}{2np_i}}}{\sqrt{2\pi np_i}} \quad \text{subject to} \quad \underline{k} \in S(n, \varepsilon), \tag{*}$$

in the sense that $\lim_{n\to\infty} \max_{\underline{k} \in S(n,\varepsilon)} |\frac{P(\underline{K}=\underline{k})}{\text{Right hand side of (*)}} - 1| = 0$.

This equation (*) appears to imply that the M components of $\underline{K}$ are asymptotically uncorrelated. However, they are actually negatively correlated with one another for all n and even in the limit $n \to \infty$. The reason why there is no contradiction here is that the formula for $P(\underline{K} = \underline{k})$ is not a product of functions of the individual components k_i because its domain is restricted to $k_1 + \cdots + k_M = n$ which is not in product form. It also should be noted that the terms in the product are not the asymptotic marginal densities of the $K_i/\sqrt{n}$; those would be $\mathcal{N}(np_i, np_i(1 - p_i))$ whereas the terms in the product in our formula are $\mathcal{N}(np_i, np_i)$. Our result can be derived either by careful, repeated applications of Stirling's formula or by deriving the asymptotic jointly normal of any $M - 1$ components of $\underline{K}/\sqrt{n}$ and then manipulating the result by replacing $k_1 + \cdots + k_{M-1}$ by $n - k_M$.

Robert A. Calderbank

A 2–adic approach to the analysis of cyclic codes

This paper describes how 2–adic numbers can be used to analyse the structure of binary cyclic codes and of cyclic codes defined over $\mathbb{Z}_{2^a}, a \geq 2$, the ring of integers modulo 2^a. It provides a 2–adic proof of a theorem of McEliece that characterizes the possible Hamming weights that can appear in a binary cyclic code. A generalization of this theorem is derived that applies to cyclic codes over $\mathbb{Z}_{2^a}$ that are obtained from binary cyclic codes by a sequence of Hensel lifts. This generalization characterizes the number of times a residue modulo 2^a appears as a component of an arbitrary codeword in the cyclic code. The limit of the sequence of Hensel lifts is a universal code defined over the 2–adic integers, which is the main subject of this paper. Binary cyclic codes and cyclic codes over $\mathbb{Z}_{2^a}$ are obtained from this universal code by reduction modulo some power of 2.

A special case of particular interest is cyclic codes over $\mathbb{Z}_4$ that are obtained from binary cyclic codes by means of a single Hensel lift. The binary images of such codes under the Gray isometry include the Kerdock, Preparata and Delsarte–Goethals codes. These are nonlinear binary codes that contain more codewords than any linear code presently

known. Fundamental understanding of the composition of codewords in cyclic codes over $\mathbb{Z}_4$ is central to the search for more families of optimal codes. This paper also constructs even unimodular lattices from the Hensel lift of extended binary cyclic codes that are self-dual with all Hamming weights divisible by 4 . The Leech lattice arises in this way as do extremal lattices in dimensions 32 through 48.

Imre Csiszár

On common randomness

The common randomness capacity of a two-terminal model is defined as the maximum rate of common randomness that the terminals can generate using resources specified by the given model. In a recent work, R. Ahlswede and the author determined this capacity for various models, including those whose statistics depend on unknown parameters. Here it is shown that a key lemma of that paper about robust uniform randomness, implies a general existence result about a function of a random variable which function is nearly uniformly distributed on a large set and is almost independent of another random variable.

As a consequence, a substantial sharpening of the wiretap channel coding theorem is obtained. Namely, the usual criterion that the wiretapper's mutual information about the sent message grows slower than linearly with the block-length, is replaced by this mutual information going to zero exponentially, and still the same secrecy capacity is obtained.

Bernhard Dorsch

High-rate unit-memory-codes

Unit-memory (UM)-codes, resp. partial-unit-memory (PUM)-codes describe convolutional codes by algebraic structures with good free distance and extended distances, especially the extended row distance, which give limits for the correctability of distributed errors. Known good decoding procedures (U. Sorger & U. Dettmar) allow promising concatenations of short, ML-decodable, inner block-codes with outer (P)UM-Codes without much delay by interleaving. One of the main problems is that outer high-rate PUM-Codes have a relatively poor free distance and UM-Codes of rate $> 1/2$ are not know. Here new construction methods for high-rate UM-Codes with good free and extended distance properties will be discussed.

Thomas Ericson and Victor Zinoviev

On Fourier invariant partitions of finite groups and Mac Williams identity for group codes

Partitions of finite abelian groups are considered. We introduce the concept of F-partition and demonstrate that this concept can be used in order to formulate very concise necessary and sufficient conditions for the existence of a Mac Williams identity with respect to a given weight function.

G. David Forney jr., Rolf Johannesson and Zhe-xian Wan

Minimal and canonical rational generator matrices for convolutional codes

A full-rank $k \times n$ matrix $G(D)$ over the rational functions $F(D)$ generates a rate-k/n convolutional code C. $G(D)$ is minimal if it can be realized with as few memory elements as any encoder for C, and $G(D)$ is canonical if it has a minimal realization in controller canonical form. We show that $G(D)$ is minimal iff for all rational input sequences $\underline{u}(D)$, the span of $\underline{u}(D)G(D)$ covers the span of $\underline{u}(D)$. Alternatively, $G(D)$ is minimal iff $G(D)$ is globally zero-free, or globally invertible. We show that $G(D)$ is canonical if and only if $G(D)$ is minimal and also globally orthogonal, in the valuation-theoretic sense of Monna.

Ernst M. Gabidulin

Metrics generated by a set of bases

A new family of metrics for coding is proposed. Let F_q^n be a vector space over the field F_q. Let $\mathcal{F} = \{\underline{f}_1, \underline{f}_2, \ldots, \underline{f}_N : \underline{f}_i \in F_q^n\}$ be a set of vectors such that: 1) $N \geq n$; 2) $\mathcal{F}$ contains n linear by independent vectors.

Definition: The $\mathcal{F}$-norm is defined by

$$N_{\mathcal{F}}(\underline{f}) = \min \#\{a_i \neq 0 : a_1, \underline{f}_1 + \cdots + a_N \underline{f}_N = \underline{f}\}.$$

The weight distribution for any $\mathcal{F}$ is found.

Some applications in communication theory and cryptology are considered.

Tor Helleseth

On exponential sums in Galois ring and applications to the weight hierarchy of Kerdock codes over Z_4

The r-th generalized Hamming weight d_r of the Z_4-linear Kerdock code is determined for $r = 0.5, 1, 1.5, 2, 2.5$. In addition it is shown that it is possible to determine the generalized weight hierarchy of the Kerdock codes of larger length using the results of d_r for a given length. We give a closed-form expression of the Lee weight of a Kerdock codeword in terms of the coefficients in its trace expansion.

Tom Høholdt and Ruud Pellikaan

Algebraic geometry codes, without algebraic geometry

Since Goppa's discovery of algebraic geometry codes a lot of effort has been put into a presentation of these codes without using the full machinery of algebraic geometry, in particular the Riemann-Roch Theorem.

We describe, by elementary means, a class of codes which includes the socalled one-point AG-codes using

1) An $\mathbb{F}_q$ algebra R

2) A weight function $g : R \to \mathbb{N}_0 \cup \{-\infty\}$

3) A surjective morphism $\varphi : R \to \mathbb{F}_q^n$

We determine the parameters of the codes and present a decoding algorithm which decodes up to half the designed minimum distance.

Henk D.L. Hollmann and Peter Vanroose

Entropy reduction, ordering in sequence spaces, and semigroups of non–negative matrices

We develope a mathematical framework to investigate classification or ordering of sequential input by means of finite–state algorithms, with the aim to reduce the "diversity" at the output, that is, to achieve entropy reduction.

Our main interest is in optimal time–varying strategies; here, given a (finite) collection of algorithms sharing a common set of internal states, we consider ordering srategies represented by sequences of this algorithms, where the action taken on the t–th input is determined by the t–th algorithm in the sequence. So in a sense we are considering a programmable finite–state device and we are looking for the best program. Surprisingly, there is a uniform method to handle questions of this type. Indeed, we first show how to transform such a problem to a problem on eigenvalues in a related semigroup of non–negative matrices, and then we present an approach to this eigenvalue problem which seems to succeed most of the time. We apply our methods to a problem concerning ordering in sequence spaces introduced by Ahlswede, Ye, and Zhang (1990), which motivated part of this work. In particular, we show that $\mathcal{T}_2(0,2,1) = \frac{1}{3}3\log(2+\sqrt{3})$, as conjectured by Peter Vanroose (co–worker on this problem) some years ago.

Rolf Johannesson, Zhe–xian Wan, and Emma Wittenmark

On systematic convolutional codes over rings

Convolutional codes over rings are motivated from phase–modulated signals.

A convolutional code is defined to be *honest* if it has an encoding matrix which has a right inverse. The definition is independent of the chosen encoding metric. All convolutional codes over finite fields are honest but there exist convolutional codes over rings which are not honest. If a $b \times c$ encoding matrix $G(D)$ has a $b \times b$ subdeterminant which is a unit in $R(G)$, the ring of rational functions, then the convolutional code encoded by $G(D)$ is honest. A convolutional encoding matrix is said to be *systematic* if it causes the information symbols to appear unchanged among the code symbols. A convolutional code over a ring R is *systematic* if it has a systematic encoding matrix. We have the following little

Proposition: A convolutional code over a ring R is systematic if and only if it has an encoding matrix, that has a $b \times b$ subdeterminant which is a unit in $R(D)$.

Our proposition is equivalent to a result by Massey and Mittelholzer [1].

[1] J.L. Massey and T. Mittelholzer, "Systematicity and Rotational Invariance of Convolutional Codes over Rings", Proc. 2nd Int. Workshop on Alg. and Combinatorial Coding Theory, Leningrad, Sept. 16–22, 1990.

Levon H. Khachatrian and Rudolf Ahlswede

Optimal anticodes

1. A system of sets $\mathcal{A} \subset \binom{[n]}{k}$ is called t–intersecting , if $(A_1 \cap A_2) \geq t$ for all $A_1, A_2 \in \mathcal{A}$, and $I(n,k,t)$ denotes the set of all such systems. Let

$$M(n,k,t) \triangleq \max_{\mathcal{A} \in I(n,k,t)} |\mathcal{A}|, 1 \leq t \leq k \leq n.$$

Let $\mathcal{F}_i \triangleq \left\{F \in \binom{[n]}{k} : |F \cap [1, t+2i]| \geq t+i\right\}$ for $0 \leq i \leq \frac{n-t}{2}$.

Theorem: For $1 \leq t \leq k \leq n$ with

(i) $(k-t+1)\left(2+\frac{t-1}{r+1}\right) < n < (k-t+1)\left(2+\frac{t-1}{r}\right)$ for some $r \in \mathbf{N}$ we have $M(n,k,t) = |\mathcal{F}_r|$, and $\mathcal{F}_r$ is up to permutations the unique optimal.

(ii) $(k-t+1)\left(2+\frac{t-1}{r+1}\right) = n$ for $r \in \mathbf{N} \cup \{0\}$ we have $M(n,k,t) = |\mathcal{F}_r| = |\mathcal{F}_{r+1}|$ and an optimal system equals — up to permutations — either $\mathcal{F}_r$ or $\mathcal{F}_{r+1}$.

2. For a Hamming space (X_α^n, d_H) , the set of n–length words over the alphabet $X_\alpha = \{0, 1, \ldots, \alpha-1\}$, we determine the maximal cardinality of subsets with a prescribed diameter d or in another language, anticodes with distance d .

Torleiv Kløve and Tor Helleseth

On the weight hierarchy of product codes

Barbers and Tena recently proved a conjectured expression for the weight hierarchy of the product of two codes satisfying the chain condition.

Using this result we have determined the weight hierarchy of some products:

simplex code $\otimes$ simplex code

simplex code $\otimes$ 1–order Reed–Muller code

1–order Reed–Muller code $\otimes$ 1–order Reed–Muller code.

János Körner

Zero–error information theory

1.) We show that the only number k for which no Hamming space can be partitioned into k Hamming spheres is $k = 3$. Furthermore, we conjecture that among the numbers ℓ for which $\{0,1\}^n$ can be partitioned into ℓ Hamming spheres there is a gap, in

the sense that the smallest ℓ larger than 2 for which such a partition is possible is $\ell = n + 2$. (joint work with Emanuela Fachini.)

2.) We get a new upper bound for the Sperner capacity of arbitrary digraphs in terms of a new entropy notion for digraphs. This concept generalizes the concept of graph entropy due to the author (1973).

Vladimir I. Levenshtein

Random Boolean functions, designs, and codes

A system of Boolean functions in n variables is called randomized if the functions preserve the property of their variables to be independent and uniformly distributed random variables. Such a system is referred to as t–resilient if for any substitution of constants for any i variables, where $0 \le i \le t$, the derived system of functions in $n - i$ variables will be also randomized. We investigate the problem of finding the maximum number $N(n,t,T)$ of functions in n variables of which any T form a t–resilient system. This problem is reduced to the minimization of the size of certain combinatorial designs, which we call split orthogonal arrays. We extend some results of design and coding theory, in particular, a duality in bounding the size of codes and designs, in order to obtain upper and lower bounds on $N(n,t,T)$. In some cases this gives rise to final results.

Jacobus H. van Lint, Henk D.L. Hollmann, and Ludo Tolhuizen

On codes with the identifiable parent property

Let C be a code of length n over an alphabet $\mathcal{D}$ of size q. For any two codewords $\underline{a}, \underline{b}$, we define the *set* of *descendants* $\mathcal{D}(\underline{a}, \underline{b})$ by

$$\mathcal{D}(\underline{a}, \underline{b}) := \{\underline{x} \in Q^n : x_i \in \{a_i, b_i\}, i = 1, 2, \ldots, n\}.$$

For a code C, we define the descendant code C^* by

$$C^* := \bigcup_{\underline{a} \in C, \underline{b} \in C} \mathcal{D}(\underline{a}, \underline{b}).$$

Since $\underline{a}$ and $\underline{b}$ are in $\mathcal{D}(\underline{a}, \underline{b})$, we have $C \subseteq C^*$.

We say that C has the "identifiable parent property" (IPP) if for every $\underline{c} \in C^*$ there is a codeword $\pi(\underline{c}) \in C$ such that

$$[\underline{c} \in \mathcal{D}(\underline{a}, \underline{b}), \underline{a} \in C, \underline{b} \in C] \Rightarrow [\pi(\underline{c}) \in \{\underline{a}, \underline{b}\}].$$

We define

$$F(n,q) := \max\{|C| : C \subseteq Q^n, |Q| = q, C \text{ has } IPP\}.$$

We present the following results:

(1) $F(1,q) = F(2,q) = q$ (easy exercise)

(2) $F(3,q) = 3q + o(q)$

(3) $F(4,q) \geq q\sqrt{q} + o(q)$, Conjecture $F(4,q) \leq q\sqrt{q}$.

(4) $q^2 \leq F(5,q) \leq 3q^2$ for $q \geq 7$

(5) $F(n,q) \leq 3q^{\lceil \frac{n}{3} \rceil}$

(6) $F(n,q) \geq c \cdot \left(\frac{q}{4}\right)^{\frac{n}{3}}$

Simon Litsyn

New upper bounds for self–dual codes

Using a variant of the linear programming method we derive a new upper bound on the minimum distance d of doubly–even self–dual codes of length n . Asymptotically it reads $\delta = d/n \leq 0.166315\ldots$, thus improving on the Mallows–Odlyzko–Sloane bound, $\delta \leq 1/6$. To establish this we prove that in any doubly–even self–dual code the distance distribution is asymptotically upperbounded by the corresponding normalized binomial distribution in the interval $[cn, (1-c)n]$ where c is $\frac{1}{2} - \sqrt{\frac{6\delta - 1 + \sqrt{1 - 8\delta + 32\delta^2}}{8(1-\delta)}}$

Hans–Andrea Loeliger

On Jaynes' proof of the second law

A concise and general proof of the second law of thermodynamics was given by Jaynes. Disregarding some details, the argument is as follows. Let $\mathcal{W} = \mathbb{R}^n$ be the phase space of some physical system. (we assume classical mechanics.) For $x \in W$, let $g(x)$ be the "macroscopic state" of the system. For $x \in W$, let $[x]_g \triangleq \{x' \in W : g(x') = g(x)\}$.

Definition: $H_g(x) \triangleq \log \mathrm{Vol}([x]_g)$.

Let $f : W \to W : x(t_0) \to x(t_1)$ be the evolution of the system according to the laws of mechanics.

Theorem: If (i) f is volume–preserving and (ii) $x' \in [x]_g \Rightarrow f(x') \in [f(x)]_g$ then
$H_g(x) \leq H_g(f(x))$.

Condition (i) is satisfied for any Hamiltonian (Liouville's theorem).

Condition (ii) is satisfied for any *reproducible* experiment.

James L. Massey and Shirlei Serconek

Linear complexity of sequences with arbitrary period

Suppose $s_0, s_1, s_2, \ldots$ is an N–periodic (i.e., $s_i = s_{i+N}$ for all $i \geq 0$) sequence over $GF(p^\mu$ where $N = p^\nu n$ and $\gcd(n,p) = 1$. The linear complexity L of this sequence is the degree of the polynomial $C(d) = 1 + c_1 D + \cdots + c_2 D^L$ such that $S^N(D)C(D) = P(D)(1 - D^N)$ where $S^N(D) = s_0 + s_1 D + \cdots + s_{N-1} D^{N-1}$ and $\gcd(C(D), P(D)) = 1$.

But $(1-D)^N = (1-D^M)P^\nu$. If α is a primitive N–th root of unity in (an extension of) $GF(p^\nu)$, it follows that the multiplicity m_i of α^i as a zero of $C(D)$ is $m_i = 0$ if and only if α^i is a zero of $S^N(D)$ of multiplicity at least p^ν and is $m_i(> 0)$ if and only if α^i is a zero of $S^N(D)$ of multiplicity $p^\nu - m_i$. Letting $S^{N[i]}(D)$ denote the i–th Hasse derivative of $S^N(D)$, it follows that $L = m_0 + m_1 + \cdots + m_{n-1}$ is the "active area" (i.e., the number of non–zero entries or entries below non–zero entries) of the matrix whose $(i+1)^{st}$ column is $\left(S^N(\alpha^i), S^{N[1]}(\alpha^i), \ldots, S^{N[p^\nu-1]}(\alpha^i)\right)$ for $0 \le i < n$. This is equivalent to a result proved recently by Ch. Gunther.

Edward C. van der Meulen and V.V. Prelov

Asymptotics of Fisher information under weak perturbation and an asymptotic generalization of De Bruijn's identity

An asymptotic expression is derived for the Fisher information of the sum Y of two independent random variables X and Z_ϵ , when Z_ϵ is small. This asymptotic expression is valid under some regularity conditions on the probability density function of X and conditions on the moments of Z . The first term of the expansion is the Fisher information of X . Higher order terms of the expansion are calculated as well. A statistical example can be given concerning the asymptotic efficiency of an unbiased estimator in a certain parametric model. Using the main result for the case $Z_\epsilon = \epsilon Z$, an asymptotic generalization of De Bruijn's identity is obtained, which provides a relationship between differential entropy and Fisher information. When Z has a Gaussian distribution with unit variance, X has a probability density function with finite variance, and X and Z are independent, then De Bruijn's identity in integral form states that

$$h(X+\varepsilon Z) - h(X) = \frac{1}{2}\int_0^{\varepsilon^2} J(X+\eta Z)d\eta^2,$$

where $J(X)$ denotes Fisher information. We obtain that for non–Gaussian Z , with all moments of Z of order up to and including m coinciding with the corresponding moments of a Gaussian distribution, the following generalization of De Bruijn's identity holds

$$h(X+\varepsilon Z) - h(X) = \frac{1}{2}\int_0^{\varepsilon^2} J(X+\eta Z)d(\eta^2) + 0(\varepsilon^m).$$

Thomas Mittelholzer

Fast maximum–likelihood decoding of group codes from finite reflection groups

Slepian–type group codes generated by finite Coxeter groups are considered. From the exceptional finite reflection groups new high rate codes with excellent distance properties are obtained. The decoding regions for maximum–likelihood decoding are explicitly characterized and an efficient ML–decoding algorithm is presented.

Prakash Narayan, A. Kanlis and S. Khudanpur

Typicality of a good rate–distortion code

We consider a good code for a discrete memoryless source with a specified distortion level to be one whose rate is close to the corresponding rate–distortion function and which, with large probability, reproduces the source within the allowed distortion level. We show that any good code must contain an exponentially large set of codewords, of effectively the same rate, which are all typical with respect to the output distribution induced by the rate–distortion achieving channel. Furthermore, the output distribution induced by a good code is asymptotically singular with respect to the i.i.d. output distribution induced by the rate–distortion achieving channel. However, the normalized (Kullback–Leibler) divergence between these output distributions converges to the conditional entropy of the output under the rate–distortion achieving channel.

Alon Orlitsky

A pair of preposterous product problems

We show that the AND and OR products of graphs are special cases of a general hypergraph product arising naturally in problems combining source coding (with and without side information) and quantization.

Via the "book critic" problem, we show that for all ε (however small) and all δ (however large) there is a quantization problem where one instance requires $\geq \delta$ bits but repeated indep. instances require $\leq \varepsilon$ bits/instance. (This extends results with N. Alon.)

We describe the chromatic entropy $H_X(G)$ of a probabilistic graph and show that $\frac{1}{n}H_X(G^k) \to H_K(G)$, the graph entropy of G. We mention results showing that for large classes of graphs, $H_K \geq H_X - \log e$ and that for some graphs $H_K \leq H_X - \log H_X - \log e$. We end by mentioning a few ideas in proving that this is the largest possible discrepancy.

Mark Pinsker and Leonid A. Bassalygo

Codes detecting localized errors

We found the asymptotically optimal rate of a code which detects the linearly increasing number $t = \tau n$, $0 < \tau < 1$ of localized errors:

$$R_{opt} = 1 - \tau.$$

Ralph–Hardo Schulz

Check digit systems with error correction

Check digit systems are systematic block codes with one or two check characters which allow to detect single errors, neighbour transpositions
(that are errors of the form $a_1 \dots a_i a_{i+1} \dots a_N \to a_1 \dots a_{i+1} a_i \dots a_N$) or double errors.

By Sethi, Rajaraman and Kenjale (1978) it is clear that detection of double errors and correction of single errors and neighbour transpositions are possible with the same code. We are able to generalize the results of Sethi et al from $\mathbb{Z}_p$ to finite abelian groups and to show the following theorem.

Theorem: Let $(A,+)$ be a finite abelian group with $\beta_i, \gamma_i \in Aut\, A$ and $\gamma_{n+2}\beta_{n+2} = \beta_{n+2}\gamma_{n+2}$ such that there exists the inverse of $\gamma_{n+2}\beta_{n+1} - \beta_{n+2}\gamma_{n+1}$. The check digit system

$$A^n \to A^{n+\ell} \text{ with } a_1 \dots a_n \to a_1 \dots a_n a_{n+1} a_{n+2} \text{ and } \sum_{i=1}^{n+2} \beta_i(a_i) = 0 = \sum_{i=1}^{n+2} \gamma_i(a_i)$$

is double error detecting and single error and neighbour transposition correcting if the following conditions are fulfilled:

(1) $\beta_i \gamma_i^{-1} \gamma_j \beta_j^{-1}$ is fixed point free on A for $i < j \leq n+2 = N$

(2) $\beta_{i+1} - \beta_i$, $\gamma_{i+1} - \gamma_i$ and $\beta_j \gamma_j^{-1}(\gamma_{i+1} - \gamma_i)(\beta_{i+1} - \beta_i)^{-1} - 1$ are invertible for $i = 1, \dots, n+1$ and $j = 1, \dots, n+2$. (Here 1 denotes the identity automorphism.)

(3) $(\beta_{j+1} - \beta_j)(\gamma_{j+1} - \gamma_j)^{-1}(\gamma_{i+1} - \gamma_i)(\beta_{i+1} - \beta_i)^{-1}$ operates fixed point freely on A for all i, k with $i < k \leq n+1$. If $|A| = p^t$ with $p \neq 2$ prime we can give examples as long as $N \leq \frac{q-1}{2}$.

Shlomo Shamai (Shitz), Sergio Verdu and Ram Zamir

Communication with systematic transmission

We investigate the information theoretic aspects of "systematic" communication, where the raw data, analogue or digital, is transmitted over the channel unencoded. Additional resources such as power, bandwidth, supplementary or shared channels, over which full encoding is allowed, are used to either reduce the average distortion below that provided by the unencoded systematic link and/or increase the rate of the transmissable information. This generic model emerges in many applications where the unencoded link is to be retained while attempting to enhance the communication capabilities of the system, exploiting the additional resources.

The achievable average distortion in this model is fully characterized and the conditions under which the unencoded link *does not* incur loss of optimality are identified and explicitly stated.

This framework extends the results by Shamai and Verdu, where fully reliable communication (zero average distortion) is at focus. In the model here, the Wyner–Ziv rate distortion function plays a fundamental role, paralleled to that fulfilled by the Slepian–Wolf source coding for the zero average–distortion case.

The results are demonstrated for a Gaussian bandlimited source and a Gaussian channel where the invariance of the bandwidth–SNR (in d_β) product is established, and where optimality of the systematic transmission is demonstrated. A binary Bernoulli source transmitted over a binary symmetric or a Gaussian channel is considered. Discussed is also an overlayed uncoded/coded communication of a Bernoulli source over a single Gaussian channel where no additional power or bandwidth are available. It is demonstrated that in

all the Bernoulli source cases described here, systematic transmission *does incur loss of optimality*, but for the extreme situation of zero average distribution [Shamai–Verdu].

Paul C. Shields

Lower bounds via coding

For each $n \geq 1$ let $\ell_n(\cdot)$ be the length function of a prefixcode on A^n, where $|A| < \infty$. Let P be a probability measure on A^∞

Lemma: (Barron) $\ell_n(X_1^n) + \log P(X_1^n) \geq -2 \log n$ eventually a.s.

Corollary: If P is ergodic with entropy H then $\liminf \frac{\ell_n(X_1^n)}{n} \geq H$, a.s.

Application 1 (String matching): Let $L(X_1^n)$ be the length of the longest string that appears at least twice in X_1^n. Assume P has finite energy, that is, $\exists K$, $0 < c < 1$ such that $P(X_{t+1}^{t+m} | X_1^t) \leq K c^m$. Then $\exists D$ such that $L(X_1^n) \leq D \log n$, eventually a.s.

Application 2: Eventually almost surely if $X_1^n = a(1)V(1)a(2)V(2)\ldots a(t)V(t)a(t+1)$ where $\ell(V(i)) \geq \frac{\log n}{H}(1+\varepsilon)$ and each $V(i)$ appears earlier then $\Sigma \ell(V(i)) \leq \varepsilon n$.

Application 3: If $q_k(\cdot|X_1^n) =$ empirical k–block distribution and $n \geq 2^{kH}$ then eventually almost surely any set $B \subset A^k$ of size almost $2^{k(1+\varepsilon)}$ satisfies $q_k(B|X_1^n) < \varepsilon$.

Yuri Shtarkov and J. Justesen

Combinatorial entropy of discrete images

The existence of such entropy is proved for the case, when the only known properties of the image source are arbitrary stationary (invariant to shift) constraints of values of picture elements. The bounds of combinatorial entropy are discussed.

Juriaan Simonis

Almost affine codes, ideal secret sharing schemes, and MacWilliams identities

An almost affine code is a code C with the property that the size of all codes obtained by multiple puncturing of C is a power of a fixed integer. Almost affine codes are more or less the same as ideal secret sharing schemes. An interesting tool in the analysis of their properties is a kind of MacWilliams equations.

Gábor Simonyi

Recovering set systems

$(A, B) \subseteq 2^{[n]}$ is a recovering pair if

(i) $A \setminus B = A' \setminus B' \Rightarrow A = A' \quad \forall A, A' \in \mathcal{A}$, $\forall B, B' \in \mathcal{B}$ and

(ii) $B \setminus A = B' \setminus A' \Rightarrow B = B' \quad \forall A, A' \in \mathcal{A}\ ,\ \forall B, B' \in \mathcal{B}\ .$

It is a several year old conjecture that for a recovering pair $(\mathcal{A}, \mathcal{B})$ one has $|\mathcal{A}||\mathcal{B}| \leq 2^n$. Here we consider the uniform version of the problem where all elements of $\mathcal{A}$ and $\mathcal{B}$ have size k for some fixed k . The optimal configuration in this case is given and is similar to the one conjectured to be optimal in the non–uniform case. Furthermore, we generalize the problem in the following way. Let G be a graph on $\{1, 2, \ldots, m\}$, and $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m \leq 2^{[n]}$ be assigned to its vertices. They form a recovering family for G if $(\mathcal{A}_i, \mathcal{A}_j)$ is a recovering pair whenever $\{i, j\} \in E(G)$. This defines new graph invariants for both the uniform and the non–uniform case. It turns out that the new invariant in the uniform case is intimately related to an old invariant, namely graph entropy.

Ludo Tolhuizen

Diamond codes

We present a new method for combining two error–correcting codes, C_1 and C_2 . The code so obtained, called Diamond code, enjoys both the error correcting capabilities of product codes and the small memory requirements of CIRC, the code applied in the Compact Disc system.
A word of the Diamond code is represented as a strip with all columns in C_1 and all diagonals (lines with a slope of 45 degrees) in C_2 . Encoding is non–trivial, as a finite number of non–zero information symbols may result in an infinite number of non–zero parity symbols. We show that for conveniently chosen C_1 and C_2 (e.g. both shortened Reed–Solomon codes), this undesirable infinite impulse response behaviour does not occur. We discuss block variations of these codes. One of these versions is a cylinder code, consisting of all matrices of given width with all columns in C_1 and all diagonals, when folded back cyclically, in C_2 . Some results on the dimension of cylinder codes are given.

Peter Vanroose and Miklós Ruszinkó

The collision channel with multiplicity feedback

Consider the following communication situation, which is commonly called the (slotted) *multiple-access collision channel*:

An unlimited number of users are allowed to transmit packets of a fixed length whose duration is taken as a time unit. A *slot* is a time interval $[t, t+1)$, where $t \in \{0, 1, 2, 3 \ldots\}$. All users send their packets through a common channel, such that each packet falls in exactly one slot. There is a single common receiver. Senders of different packets cannot interchange information. The packet arrival times are modeled as a Poisson process in time with intensity λ .

When two or more users send a packet in the same time slot, these packets "collide" and the packet information is lost, i.e., the receiver cannot determine the packet contents, and retransmission will be necessary. However, all users can learn — from the *feedback* just before time instant $t + 1$ — the multiplicity of the collision in time slot $[t, t + 1)$. Thus, multiplicity 0 means an idle slot, multiplicity 1 means successful transmission by a single user, while multiplicity > 1 means that retransmission will be necessary.

A *conflict resolution protocol* is a retransmission scheme for the packets in a collision. Such a scheme must insure the eventual successful transmission of all these packets.

Clearly, because of the Poisson arrival of messages, i.e., of new users, message packets waiting for transmission will accumulate during the epoch. These packets will all be transmitted in the time slot following the epoch.

It is of course important that the maximum transmission delay, i.e., the maximal expected time between the generation and the successful transmission of a given packet, must be finite. The supremum of the set of intensities λ for which a certain protocol still gives raise to a finite delay is called its *throughput*. The *capacity* of a certain collision channel is the supremum of achievable throughputs, taken over all possible protocols.

A good overview on collision channels can be found in the special issue of March 1995 of the IEEE Transactions on Information Theory. For the collision channel without feedback, Massey and Mathys proved in that issue that the capacity is $1/e = 0.36788$. In the "classical" situation of binary feedback (collision/no collision), the capacity is still unknown; the best lower bound is 0.48775, the best upper bound 0.587.

Pippenger showed in 1981 (IEEE-IT–27(2):145–151) in a probabilistic way that the capacity of a collision channel with multiplicity feedback is one. Since then, no constructive proof of this result was given. We have now derandomized Pippenger's proof, and also provide an absolute upper bound on the expected packet delay, which only depends on λ .

We modify Pippenger's protocol in the following way: instead of having a single 'detecting' matrix for a given number k of 'active' users, which corresponds to a parallel search strategy for the identifiers, we first split the users into $k/\log k$ groups and then have a 'detecting' matrix for each group separately, i.e., a two-step adaptive search. While no construction exists for the detecting matrices used by Pippenger, we can use the detecting matrices constructed by Lindström in 1965 (Can. Math. Bull. 8(4): 477–490).

We prove that the expected packet delay is upper bounded by $128e^2 f(\lambda)/(1-\lambda)$, where $f(\lambda) = \sum_t t \log\log t/\log t$, and where the sum extends to the value of t for which $\log\log t/\log t < (1-\lambda)/(32\lambda)$.

Sergio Verdu

The exponential distribution in information theory

It is shown that the exponential distribution leads to information theoretic formulas which are strikingly similar to their Gaussian counterparts:

- A saddle–point property satisfied by the mutual information between a random variable and its sum with an exponential random variable.
- Rate–distortion function of the Poisson process.
- Capacity of single–user and multiaccess channels with additive exponential noise.
- Capacity of Controlled Markov Processes.

Zhe-xian Wan

On the uniqueness of the Leech lattice

It was found that there is an error in Venkov's proof of the uniqueness of the Leech Lattice. A construction of neighbours of even unimodular lattices is given and is used to modify Venkov's proof so that the error can be corrected.

Jan Willems

Representation of linear systems

Let $\mathbb{F}$ be a finite field, or $\mathbb{R}$, or $\mathbb{C}$. We will call a behaviour, i.e., a subset of $(\mathbb{F}^q)^{\mathbb{Z}}$, a convolutional code if it is linear, shift-invariant and complete (meaning that $w \in \mathcal{B}$ iff $w|_{[t_0,t_1]} \in \mathcal{B}|_{[t_0,t_1]} \forall t_0, t_1 \in \mathbb{Z}$).

Let $\mathcal{R} \in \mathbb{R}^{\cdot \times q}[\xi, \xi^{-1}]$ and denote by D the delay. Consider the set of difference equations $\mathcal{R}(D, D^{-1})w = 0$. The set of solutions defines a convolution code and conversely, every convolutional code can be obtained this way. We will call this a kernel representation and the rows of $\mathcal{R}$ are called syndrome formers.

There exist many other representations and specifications of convolutional codes. Let us just mention one of them. We have just seen that every convolutional code is the kernel of a polynomial operator in D. Is it also the image of such an operator? The answer is yes, provided the code is controllable, i.e., if $w_1, w_2 \in \mathcal{B}$ implies the existence of a $w \in \mathcal{B}$ and $\tau > 0$ such that $w(t) = w_1(t)$ for $t < 0$ and $w(t - \tau) = w_2(t)$ for $t \geq \tau$.

Jacob Ziv and Neri Merhav

On the amount of statistical side information required for lossy data compression

Consider a vector quantizer that is equipped with N side information bits of an arbitrary representation of the statistics of the input source. We investigate the minimum value of N such that the rate–distortion performance of this quantizer would be essentially the same as the optimum quantizer for the given source.

Berichterstatter: B. Balkenhol, U. Tamm

Tagungsteilnehmer

Prof.Dr. Rudolf Ahlswede
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131

33501 Bielefeld

Prof.Dr. Richard E. Blahut
Coordinated Science Laboratory
University of Illinois
1308 W. Main Street

Urbana , IL 61801
USA

Prof.Dr. Vladimir Balakirsky
Data Security Association Confident
Smolny

193060 St. Petersburg
RUSSIA

Prof.Dr. Martin Bossert
Abteilung Informationstechnik
Universität Ulm
Albert-Einstein-Allee 43

89081 Ulm

Dr. Bernhard Balkenhol
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131

33501 Bielefeld

Prof.Dr. Jehoshua Bruck
Computation & Neural Systems
and Electrical Engineering
Caltech, 116 - 81

Pasadena , CA 91125
USA

Prof.Dr. Leonid A. Bassalygo
Institute for Information Trans-
mission Problems
Russian Academy of Sciences
19 Bol.Karetny per,

101447 Moscow GSP-4
RUSSIA

Prof.Dr. Mazat V. Burnashev
Institute for Problems of
Information Transmission
Russian Academy of Sciences
Ermolova 19

101447 Moscow GSP-4
RUSSIA

Prof.Dr. Toby Berger
Dept. of Electrical Engineering
Cornell University
Rhodes Hall

Ithaca , NY 14853
USA

Prof.Dr. A. Robert Calderbank
AT&T Labs-Research
PO Box 971
180 Park Avenue

Florham Park , NJ 07932-0971
USA

Prof.Dr. Imre Csiszar
Mathematical Institute of the
Hungarian Academy of Sciences
P.O. Box 127

H-1364 Budapest

Prof.Dr. Joachim Hagenauer
Institut für Nachrichtentechnik
Technische Hochschule München
Arcisstr. 21

80333 München

Prof.Dr. Bernhard Dorsch
Institut für Netzwerk- und
Signaltheorie
TH Darmstadt
Merckstr. 25

64283 Darmstadt

Prof.Dr. Tor Helleseth
Department of Informatics
University of Bergen
Hoyteknologisenteret

N-5020 Bergen

Prof.Dr. Thomas Ericson
Dept. of Electrical Engineering
Division of Data Transmission
Linköping University

S-58183 Linköping

Prof.Dr. Tom Hoholt
Matematisk Institut
Danmarks Tekniske Hojskole
Bygning 303

DK-2800 Lyngby

Dr. David Forney
Codex Corporation
20, Cabot Boulevard

Mansfield , MA 02048-1193
USA

Prof.Dr. Henk D.L. Hollmann
Philips Research Laboratories
Room WY 8.56

NL-5656 AA Eindhoven

Prof.Dr. Ernst M. Gabidulin
Chair of Higher Mathematics
Moscow Physical-Technical Institute
Institute by Street 9

141700 Dolgoprudnyi , Moscow Region
RUSSIA

Prof.Dr. Rolf Johannesson
Dept. of Information Theory
University of Lund
Box 118

S-221 00 Lund

Prof.Dr. Levon H. Khachatrian
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131

33501 Bielefeld

Prof.Dr. Simon N. Litsyn
Dept. of Electrical Engineering
Systems
Tel Aviv University

Ramat Aviv 69978
ISRAEL

Prof.Dr. Torleiv Klöve
Department of Informatics
University of Bergen
Hoyteknologisenteret

N-5020 Bergen

Prof.Dr. Hans-Andrea Loeliger
Dept. of Electrical Engineering
Linkoeping University

S-581 83 Linkoeping

Dr. Janos Körner
Dept. of Computer Sciences
Universita "La Sapienza"
Via Salaria 113

I-00198 Roma

Prof.Dr. James L. Massey
Inst. f. Signal- und Informations-
verarbeitung
ETH Zürich
Gloriastr. 35

CH-8092 Zürich

Prof.Dr. Vladimir I. Levenshtein
M.V. Keldysh Institute of Applied
Mathematics
Russian Academy of Sciences
Miusskaya pl. 4

125047 Moscow
RUSSIA

Prof.Dr. Edward C. van der Meulen
Kath. Univ. Leuven
Dept. of Math.
Celestijnenlaan 200B

B-3030 Heverlee

Prof.Dr. Jacobus H. van Lint
Dept. of Mathematics and
Computing Science
Eindhoven University of Technology
Postbus 513

NL-5600 MB Eindhoven

Dr. Thomas Mittelholzer
Inst. f. Signal & Info. Processing
ISI ETF F103
ETH-Zentrum

CH-8092 Zürich

Prof.Dr. Prakash Narayan
Electrical Engineering Department
College of Engineering
University of Maryland

College Park , MD 20742
USA

Prof.Dr. Shlomo Shamai
Dept. of Electrical Engineering
TECHNION
Israel Institute of Technology

Haifa 32000
ISRAEL

Prof.Dr. Alon Orlitzky
AT & T Bell Laboratories
P.O. Box 636
600 Mountain Avenue

Murray Hill , NJ 07974-2070
USA

Prof.Dr. Paul C. Shields
Dept. of Mathematics
University of Toledo
2801 W. Bancroft St.

Toledo , OH 43606-3390
USA

Prof.Dr. Ruud Pellikaan
Dept. of Mathematics & Comp.Science
Eindhoven University of Technology
Geb. 9.86
P.O. Box 513

NL-5600 MB Eindhoven

Prof.Dr. Yuri Shtarkov
Institute for Problems of
Information Transmission
Russian Academy of Sciences
Ermolova 19

101447 Moscow GSP-4
RUSSIA

Prof.Dr. Mark S. Pinsker
Institute for Information Trans-
mission Problems
Russian Academy of Sciences
19 Bol.Karetny per,

101447 Moscow GSP-4
RUSSIA

Prof.Dr. Juriaan Simonis
Dept. of Mathematics and
Computer Science
Delft University of Technology
P. O. Box 5031

NL-2600 GA Delft

Prof.Dr. Ralph-Hardo Schulz
Institut für Mathematik II (WE2)
Freie Universität Berlin
Arnimallee 3

14195 Berlin

Prof.Dr. Gabor Simonyi
Mathematical Institute of the
Hungarian Academy of Sciences
P.O. Box 127
Realtanoda u. 13-15

H-1364 Budapest

Dr. Ulrich Tamm
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131

33501 Bielefeld

Prof.Dr. Adrianus J. Vinck
Institut für Experimentelle
Mathematik
Universität-Gesamthochschule Essen
Ellernstr. 29

45326 Essen

Prof.Dr. Ludo Tolhuizen
Philips Research Laboratories
Room WY82
Prof. Holstlaan 4

NL-5656 AA Eindhoven

Prof.Dr. Zhe-Xian Wan
Department of Information Theory
Lund University
Box 118

S-22100 Lund

Prof.Dr. Peter Vanroose
ESAT-MI2
Katholieke Universiteit Leuven
Kard. Mercierlaan 94

B-3001 Heverlee

Prof.Dr. Jan C. Willems
Mathematisch Instituut
Rijksuniversiteit Groningen
Postbus 800

NL-9700 AV Groningen

Prof.Dr. Alexander Vardy
Coordinated Science Laboratory
University of Illinois at
Urbana-Champaign
1101 W. Springfield Avenue

Urbana , IL 61801
USA

Prof.Dr. Victor A. Zinovjev
Date Transmission
Dept. of Electrical Engineering
Linkoping University

S-58183 Linkoping

Prof.Dr. Sergio Verdu
Dept. of Electrical Engineering
Princeton University
Engineering Quadrangle

Princeton , NJ 08544
USA

Prof.Dr. Jacob Ziv
Dept. of Electrical Engineering
TECHNION
Israel Institute of Technology

Haifa 32000
ISRAEL

EMAIL-ADRESSEN

Ahlswede, Rudolf	hollmann@mathematik.uni-bielefeld.de
Balakirsky, Vladimir	vbal@mathematik.uni-bielefeld.de
	vbal@stoic.spb.su
Balkenhol, Bernhard	bernhard@mathematik.uni-bielefeld.de
Bassalygo, Leonid	bass@ippi.ac.msk.su
Berger, Toby	berger@ee.cornell.edu
Blahut, Richard E.	blahut@shannon.csl.uiuc.edu
Bruck, Jehoshua	bruck@paradise.caltech.edu
Burnashev, Marat V.	burn@ippi.ac.msk.su
Calderbank, Robert A.	rc@research.att.com
Csiszar, Imre	csi@math-inst.hu
Dorsch, Bernhard	dorsch@nesi.e-technik.th-darmstadt.de
Ericson, Thomas	thomas@isy.liu.se
Forney, G. David Jr.	luse27@email.mot.com
Gabidulin, Ernst M.	gab@re.mipt.su
	gab@ippi.ac.msk.su
Hagenauer, Joachim	hag@lnt.e-technik.tu-muenchen.de
Helleseth, Tor	torh@ii.uib.no
Hollmann, Henk D. L.	hollmann@natlab.research.philips.com
Hoholdt, Tom	tom@mat.dtu.dk
Johannesson, Rolf	rolf@dit.lth.se
Khachatrian, Levon	lk@mathematik.uni-bielefeld.de
Klove, Torleiv	torleiv@ii.uib.no
Koerner, Janos	korner@dsi.uni-roma1.it
Levenshtein, Vladimir	leven@applmat.msk.su
	vladimir@ii.uib.no
Litsyn, Simon	litsyn@eng.tau.ac.il
van Lint, Jacobus H.	wsdwjhvl@urc.tue.nl
Loeliger, Hans-Andrea	andi@isy.liu.se
Massey, James L.	massey@isi.ee.ethz.ch
Mittelholzer, Thomas	mittelholzer@isi.ee.ethz.ch
van der Meulen, Edward	ecvdm@gauss.wis.kuleuven.ac.be
Narayan, Prakash	prakash@eng.umd.edu
Orlitsky, Alon	alon@research.att.com
Pellikaan, Ruud	ruudp@win.tue.nl
Pinsker, Mark S.	pinsker@ippi.ac.msk.su
Schulz, Ralph-Hardo	schulz@math.fu-berlin.de
Shamai, Shlomo S.	sshlomo@ee.technion.ac.il
Shields, Paul	pshields@math.utoledo.edu
Shtarkov, Yuri	shtarkov@ippi.ac.msk.su
Simonis, Juriaan	j.simonis@twi.tudelft.nl
Simonyi, Gabor	simonyi@math-inst.hu
	simonyi@konig.elte.hu
Tamm, Ulrich	tamm@mathematik.uni-bielefeld.de
Tolhuizen, Ludo	tolhuizn@natlab.research.philips.com
Vanroose, Peter	Peter.Vanroose@esat.kuleuven.ac.be
Vardy, Alexander	vardy@golay.csl.uiuc.edu
Verdu, Segio	verdu@princeton.edu
Vinck, Han	vinck@exp-math.uni-essen.de
Wan, Zhe-xian	wan@dit.lth.se
Willems, Jan C.	J.C.Willems@math.rug.nl
Zinoviev, Victor	zinov@ippi.ac.msk.su
Ziv, Jacob	jz@ee.technion.ac.il