MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 15/1992

Informationstheorie

05.04. bis 11.04.1992

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

Folgende Themen standen im Vordergrund

- Algebraische Kodierungstheorie
- Kombinatorik auf Folgeräumen
- "Multi-User" Kodierungstheorie
- Modulation Codes
- Kommunikationskomplexität

Vortragsauszüge

Rudolf Ahlswede:

On a General Theory of Information Transfer

We live in a world vibrating with "information" and in most cases we don't know how it is processed or even what it is at the semantic and pragmatic levels. A multitude of challenges to information theory comes from computer science. They, in particular, have stimulated us to reconsider the basic assumptions of Shannon's Theory and to investigate, whether its formulation is broad enough. This theory deals with "messages", which are elements of a prescribed set of objects, known to the communicators. The receiver wants to know the true message. This basic model, occuring in all engineering work on communication channels and networks addresses a very special communication situation. More generally they are characterized by

(I) The senders prior knowledge
(II) The prior knowledge of the receiver
(III) The question of the receivers concerning the given "ensemble", to be answered by the senders.

We build up an understanding by considering first specific problems and then outline a general theory of information transfer. The classical transmission problem as formulated by Shannon and the identification problem are known special cases.

Ingo Althöfer:

Compression of Chess Games Using a Deterministic Chess Computer

The storage of chess games can be done effectively, if a deterministic chess computer is available. Mephisto Roma II, for instance, a commercial chess machine, allows to compute not only the best, but also second and third best move proposals in any position. In typical master games these computer proposals coincide with the moves played by the humans rather often: 33% 1. proposal, 18% 2. proposal, 13% 3. proposal.
These coincidences can be used in an encoding scheme with very short bit strings for the cases where the computer guesses the master moves. As an example, the first six games of the 1972 match between Spassky and Fischer take 2693 bits, if stored by the best traditional method, and only 2001 bits by our new method.
To the best of our knowledge this is the first time where a concrete product of Artificial Intelligence is used for data compression purposes.

L.A. Bassalygo:

Codes Correcting Localized Errors

A review of recent results of R. Ahlswede, L. Bassalygo, S. Gelfand, D. Gevorkjan, G. Kabatyansky, M. Pinsker about codes correcting localized errors is presented.
We suppose that during the transmission of q-ary words of length n over the channel at most t errors occur and the encoder knows the set of t positions where these errors are

possible. The decoder doesn't know anything about these positions. The code corrects t localized errors if the decoder can correctly recover every message. A code word depends not only on the message but also on the configuration of possible errors. The maximal number of messages, which we can transmit by a code correcting t localized errors, is denoted by $L_q(n,t)$. Asymptotically exact and exact values $L_q(n,t)$ are obtained for several cases.

Toby Berger:

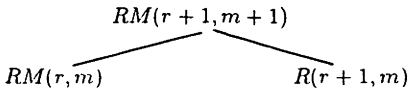
New Results in Successive Refinements

Successive refinement is said to hold when an information source first is described coarsely in an efficient manner and then can be described more finely via additional information in such a way that the total information supplied is no greater than it need have been had we proceeded directly to the fine description without the coarse one having intervened. The successive refinement problem is shown to be a special case of several multiterminal source coding problems previously considered in the literature — the Gray–Wyner model, the multiple description problem, and especially Yamamoto's cascaded sources problem to which it is proven here to be equivalent. The class of sources exhibiting succesive refinement is shown to include all Gaussian random fields with stationary measures and quadratic error, and all sources under both absolute and quadratic error whenever the Shannon lower bound to the rate–distortion function is tight at the coarse distortion. Several open problems were cited, including the general one of "how to further inform someone efficiently".

Th. Beth:

Special Group Codes: Algebra and Practice

Following the talks by Bossert, Blahut, and Ingemarsson at this conference a group theoretic approach to the construction of error–correcting codes both in the discrete (Hamming–) and real (modulation) space is given. The connection of algebraic geometry codes and generalized BCH–codes by virtue of the DFT–Mattson–Solomon approach, as described by Blahut, relies on the FFT–transform in its well–known tensorproduct decomposition of the irreducible 1 dim–group representation of the group of automorphisms, while the socalled coset decomposition leading to the classical FFT version can be applied to more cases, such as FFT (2^r) and the Hadamad transform FHT (2^r) . This especially applies to the construction of codes, which are group codes as defined by Ingemarsson, i.e. codes as orbits of isometry groups. The deep connection between these concepts is displayed by reconsidering the renowned Reed Muller Codes $RM(r,m)$ over $GF(2)$. The isometry group of $RM(r,m)$ is the Special Linear Group $SL(m,2)$. Owing to the decomposition $RM(r+1,m+1) \simeq RM(r+1,m) \oplus RM(r,m)$ the isometry groups allow an adapted coset decomposition $SL(m+1,2)/SL(m,2)$ where the subgroup $SL(m,2)$ is the canonical stabilizer of the $(m+1)$–th coordinate. Thus the tree



gives a decomposition chain of RM-codes as G-modules of the subgroup tower indicated, leading to the terminal codes $RM(0,m')$ (repetition codes) and $RM(m'-1,m')$ (parity codes) which are irreducible 1-dimensional (resp. their complements) G-Spaces, for which a fast decoding procedure has been given in Bossert's talk. It is shown that the underlying method of coded modulation is a direct consequence of the representation theoretic aspects described here.

Richard E. Blahut:

Algebraic Geometry Codes and Signal Processing

Good codes have recently been developed with the aid of algebraic geometry. Now that we know the structure of such codes, the question arises of whether they can be constructed in a more elementary way. These codes would be accessible to a wider audience if algebraic geometry could be suppressed from their development. This paper will show, with hindsight, how some of these codes can be defined in terms of Reed–Solomon codes by a construction parallel to the Turyn construction for the Golay code from Hamming codes.

M. Bossert:

Coded Modulation with Generalized Concatenation

Coded modulation combines modulation with coding in order to increase the performance of digital transmission. Coded modulation will be described as generalized concatenated codes. The inner codes are over the m-dimensional euclidean space $\mathbf{R}^m$. Using block codes of length n as outer codes a coded modulation scheme over $\mathbf{R}^{m \cdot n}$ is obtained. The construction can also be used as a multidimensional signal set and thus, the so called set partitioning can be constructed. It will be shown that the finite sections of lattices which are recently used as multidimensional signal sets can be described by generalized concatenation as well.
Furthermore, Reed–Muller codes will be described as generalized multiple concatenated codes and as a consequence of this description a soft decision decoding algorithm for these codes is derived. The ability of soft decision decoding will improve considerably the performance of decoding, also for coded modulation schemes.

A.R. Calderbank:

Linear and Nonlinear Codes for the Cyclic Triangle

Shannon introduced the concept of zero-error capacity of a discrete memoryless channel. The channel determines an undirected graph on the symbol alphabet, where adjacency means that symbols cannot be confused at the receiver. The zero–error or Shannon capacity is an invariant of this graph. Gargano, Körner, and Vaccaro have recently extended the concept of Shannon capacity to directed graphs. Their generalization of Shannon capacity is called Sperner capacity. We resolve a problem posed by these authors by giving the first example (the two orientations of the triangle) of a graph where the Sperner capacity depends on the orientation of the edges.

G. Cohen (joint work with G. Zemor):

Threshold Codes and Z–Channels

Let C be a binary linear $[n, nR, d]$ code, and let us choose randomly a vector v of length n, $v = (v_1, v_2, \ldots, v_n)$ where $Pr\{v_i = 1\} = p, \forall i$. Let $f_c(p)$ be the probability that v covers some non zero codeword of C. By a simple generalization of a result of Margulis, we show that f_c displays a threshold (T) phenomenon when n tends to ∞, provided d also goes to ∞.
We furthermore show: 1) $T \leq 1 - R$, where $T = \frac{1}{n}(f_c^{-1}(\frac{1}{2}))$. 2) For almost all codes $T = 1 - R$.
We give an illustration to coding for the Z–channel (where "1" is always correctly received, whereas "0" can be transformed into "1" with probability q); some threshold codes with rate $R = (1 - q)/2$ could be used on this channel. Highly intersecting codes (linear Sperner families with minimum size of intersection growing to ∞ with n) are good candidates. We give some constructions for them. We end the talk with open questions on the threshold of residual codes.

Bernhard Dorsch:

Error–Exponent–Estimations for Various Decoding Principles

The main point of the paper is, that what we expect and are used to in the Discrete World $\mathbf{F}_q^N$ often does not hold in the Analog World $\mathbf{R}^N$. For three main decoding principles the decoding error probability is compared, using error–exponent–estimations:
1) Bounded Minimum Distance Decoding with symmetric disjoint decision regions.
2) Threshold Decoding, with a fixed optimum threshold and symmetric, but overlapping decision regions.
3) Maximum Likelihood Decoding.
In all three cases decoding performs much differently in the analog case with AWGN and Euclidean Distances than in finite fields with Hamming Distances.

Michele Elia:

Are Fifth–Degree Equations over $GF(5^m)$ Solvable by Radicals?

The solution of algebraic equations by radicals over any field has long been a fascinating subject. Applications to algebraic decoding and to cryptography enhanced the importance of this undertaking. Here we consider fifth–degree polynomials over $GF(5^m)$ and we prove the following

i) Any polynomial can be reduced to the form $x^5 - x^2 - A$ by a Tschirnhaus transformation of the form $y = b_2x^3 + b_3x^2 + b_4x + b_5$ with at most a quadratic extension.
ii) Any polynomial $x^5 - x - a$ admits a closed–form solution.
iii) The transformation $y = -(2x^3 - x^2 + x + 3 - \frac{1}{a})/\sqrt[3]{a}$ brings $x^5 - x - a$ into $y^5 - y^2 - A$ with $A = 3(a^4 + 1)^2/\sqrt[3]{a^{20}}$
iv) There exists a Tschirnhaus transformation that brings any fully reducible or irreducible polynomial into $x^5 - x - a$, with all the coefficients of the transformation in $GF(5^m)$.

Tor Helleseth:

Nonbinary Codes meeting the Griesmer Bound

The Griesmer bound says that for any $[n,k,d]$ code over $GF(q)$, $n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$ where $\lceil x \rceil$ is the smallest integer $\geq x$. For $q=2$ and $d \leq 2^{k-1}$ it is known that all codes meeting the Griesmer bound can be obtained from the Solomon and Stiffler construction or the Belov construction.
For $q \geq 3$ and $d \leq q^{k-1}$, there are several other possible codes that meet the Griesmer bound. In particular, a construction due to Hamada, Helleseth and Ytrehus, give new nonbinary codes as follows. Let $G = [S_{k,q^\ell} \setminus F]$ be a generator matrix for a code such that S_{k,q^ℓ} denotes the columns of the generator matrix of a $\left[\frac{q^{\ell k}-1}{q^\ell - 1}, k, q^{\ell(k-1)}\right]$ simplex code over $GF(q^\ell)$ and $F = \bigcup_{i=1}^{h} V_{u_i}$ is a disjoint union of $(u_i - 1)$-flats in $PG(k-1,q)$.
We show that this is a class of $\left[\frac{q^{k\ell}-1}{q^\ell-1} - \sum_{i=1}^{h} \frac{q^{u_i}-1}{q-1}, k, q^{\ell(k-1)} - \sum_{i=1}^{h} \frac{q^{u_i} - [q^{u_i - \ell}]}{q-1}\right]$ codes which for suitable choices of $\ell, u_1, \ldots, u_h$ meet the Griesmer bound.
For $\ell = 1$ this is the class of Solomon and Stiffler codes, but for $\ell > 1$ this family is not equivalent to the Solomon and Stiffler codes.

Ingemar Ingemarsson:

Generalized Group Codes

Let Ω be the group of all distance-preserving transformations of a metric space. Let $\mathcal{G} \subset \Omega$ be a subgroup of Ω and x an element in the space. Then a Generalized Group Code is defined as the set of elements obtained by $\mathcal{G}$ operating on x.

$$\mathcal{C} = \mathcal{G}\,x$$

If $\mathcal{H} \subset \Omega$ is the stabilizer of x $(x = Hx; H \in \mathcal{H})$ then:

$$|\mathcal{C}| = |\mathcal{G}|/|\mathcal{H}|$$

Special cases are: Slepian's group codes for the Gaussian channel where the space is $\mathbf{R}^n$ and $\mathcal{G}$ a group of orthogonal matrices, linear algebraic codes where the space is F_q^n and $\mathcal{G}$ is a group of translations, permutation modulation were the space is $\mathbf{R}^n$ and $\mathcal{G}$ a group of permutation on n letters and linear codes with Lee metric where the space is Z_q^n, and $\mathcal{G}$ a group of translations. New codes are constant-weight codes (where x is binary); a special case of permutation codes which in turn is a subset of permutation modulation.

Rolf Johannesson:

On the Invariance of the Generalized Constraint Lengths
(joint work with Zhe-Yian Wan)

Let G be a $k \times n$ convolutional encoding matrix over $F(D)$. G is said to be *canonical* if it is realizable in controller canonical form with the minimum number of memory elements of any realization of any equivalent encoding matrix. Recently Forney (1991) defined the *generalized constraint lengths* for encoding matrices over $F(D)$. (For *minimal* encoding matrices over $F[D]$ this definition coincides with his (1970)–definition of constraint lengths.)
We have
Theorem: The generalized constraint lengths of two equivalent canonical encoding matrices are equal one by one up to a rearrangement.

Ref.
Forney, G.D., Jr (1970), Convolutional codes I: Algebraic structure. IEEE Trans.Inform. Theory, IT-16: 720–738.
Forney, G.D., Jr (1991), Algebraic structure of convolutional codes, and algebraic system theory. In *Mathematical System Theory*, A.C. Antoulas, Ed., pp. 527–558. Springer–Verlag, Berlin.

Torlew Klöve:

Minimum Support Weights

For an $[n,k]$ binary code C, one defines $d_r(C)$ as the smallest support of an $[n,r]$ subcode of C.
A fundamental relation is

$$(2^r - 1)d_{r-1} \leq (2^r - 2)d_r$$

for $1 < r \leq k$. Using this relation in combination with the ordinary Griesmer bound on a punctured code E we can show that

$$n \geq d_r + \sum_{i=1}^{k-r} \left\lceil \frac{d_r}{2^i(2^r-1)} \right\rceil .$$

If $n = d_1 + \sum_{i=1}^{k-1} \left\lceil \frac{d_1}{2^i} \right\rceil$, then, for all r, we have

$$n = d_r + \sum_{i=1}^{k-r} \left\lceil \frac{d_r}{2^i(2^r-1)} \right\rceil ,$$

$$d_r = \sum_{i=0}^{r-1} \left\lceil \frac{d_1}{2^i} \right\rceil ,$$

$$d_r = \left\lceil \frac{2^r-1}{2^r-2} d_{r-1} \right\rceil .$$

D.E. Lazić:

Error Exponent of any Specific Family of Block Codes

A direct, general and conceptually simple geometrical method for determining lower and upper bounds on the error exponent of any specific family of channel block codes used on a given coding channel is presented. It is considered that a specific family of codes is characterized by a unique asymptotic (in code length) expected Bhattacharyya distance distribution exponent, defined as the negative normalized logarithm of the expected Bhattacharyya distance distribution. The new method discards the well–known random coding argument used in lower–bounding the channel error exponent, enabling one to obtain the error exponent that pertains to a specific family of channel codes used on the given transmission channel. The code family that attains the channel error exponent is the optimal one, and its Bhattacharyya distance distribution the optimal distance distribution. The requirements that a code family should meet in order to attain the channel error exponent are now stated in a limpid way – the family should have the optimal Bhattacharyya distance distribution.

J.H. van Lint:

The Johnson Bound

We explain a recent result of A.E. Brower and L.M.G.M. Tolhuizen. The classical Johnson bound

$$(1)\ |C| \cdot \left\{ \sum_{i=0}^{e} \binom{n}{i} + \frac{\binom{n}{e}}{\left\lfloor \frac{n}{e+1} \right\rfloor} \left(\frac{n-e}{e+1} - \left\lfloor \frac{n-e}{e+1} \right\rfloor \right) \right\} \leq 2^n$$

for a binary code C of length n with distance $d = 2e+1$ is obtained by a counting argument from

$$|C| \cdot \left\{ \sum_{i=0}^{e} \binom{n}{i} + \frac{1}{\left\lfloor \frac{n}{e+1} \right\rfloor} \left(\binom{n}{e+1} - a_d \binom{d}{e} \right) \right\} \leq 2^n.$$

In the proof of Johnson a_d is estimated as $\binom{n}{e} / \binom{d}{e} \cdot a_{d,e}$ where $a_{d,e}$ is the number of codewords of weight d with ones in e *given* positions. This is estimated as $\left\lfloor \frac{n-e}{e+1} \right\rfloor$. The improvement is based on the observation that the sum of this many codewords would yield a codeword of a *very large* weight. This is excluded by an easy argument. The result replaces $\frac{n-e}{e+1} - \left\lfloor \frac{n-e}{e+1} \right\rfloor$ by this expression $+1$.

Katalin Marton:

On the Blowing–up Property of Stationary Processes

The "blowing–up" property (for i.i.d. processes) was introduced in a paper of Ahlswede, Gács and Körner, to prove strong converses in multi–user information theory. We explore

this property, and a stronger version of it for sources with memory. There is an evidence that this property is closely related to the ergodic theoretic properties of the process.

James L. Massey:

On Codes for the Two–User Binary Adder Channel

On the two-user binary adder channel, the received word is the real componentwise sum of the two transmitted words. The following is proved:
Theorem: Let C_1 and C_2 be blocklength n binary constant–weight codes with weights w_1 and w_2 and minimum distances d_1 and d_2, respectively. Let

$$D_{\min} = \min\{d_H(\underline{x},\underline{y}) : \underline{x} \in C_1, \underline{y} \in C_2\}$$

and

$$D_{\max} = \max\{d_H(\underline{x},\underline{y}) : \underline{x} \in C_1, \underline{y} \in C_2\}.$$

Then,

$$\max\{d_1, d_2\} + D_{\min} > D_{\max}$$

is a sufficient condition for the pair (C_1, C_2) to be uniquely decodable on the two–user binary adder channel, i.e., for $\#(C_1, C_2) = \#(C_1) \cdot \#(C_2)$.
It is further shown how to combine codes that are uniquely decodable by this theorem to produce uniquely decodable codes with $R_1 + R_2 > 1$.

H.F. Mattson, Jr.:

On Fault–Detection in Networks

To find broken links in networks we use the cut–set space. Information on which nodes can talk, or not, to which other nodes allows reduction of the problem to that of decoding the cut–set code of a graph. Special classes of such codes are known to have polynomial–time decoding algorithms. We present a simple algorithm to achieve the reduction and apply it in two examples.

E.C. van der Meulen:

Distribution Estimation Consistent in Information Divergence

We consider the problem of estimating an unknown probability distribution μ, defined on an arbitrary measurable space $(\mathcal{X}, B)$, based on i.i.d. observations $X_1, \ldots, X_n$ from μ, such that the resulting distribution estimate $\hat{\mu}_n$ is consistent in information divergence $I(\mu, \hat{\mu}_n)$. First we observe that if μ is absolutely continuous then the standard empirical measure is not suitable since then $I(\mu, \hat{\mu}_n)$ will be infinite with positive probability. In order to obtain consistency we must also limit the class of distributions to which the unknown μ belongs. As a priori information we assume that there exists a known probability measure ν such that $I(\mu, \nu) < \infty$. We introduce a

distribution estimator μ_n^* , which is a modification of the empirical measure, such that $\lim_{n\to\infty} E(I(\mu,\mu_n^*)) = 0$ and $I(\mu,\mu_n^*) \to 0$ a.s. as $n \to \infty$, under appropriate conditions. This distribution estimator is further applied to design a universal source code for finely quantized data. It is shown that the redundancy of such a code tends to zero uniformly in partitions for all μ such that $I(\mu\nu) < \infty$. The results are contained in the following paper:
A.R. Barron, L. Györfi, and E.C. van der Meulen: "Distribution estimation cosistent in total variation and in two types of information divergence", IEEE Trans. on Information Theory, 1992 (to appear).

Thomas Mittelholzer:

Convolutional Codes over Groups

The motivation to consider convolutional codes over groups rather than over fields comes from the fact that there are nonabelian groups corresponding to signal sets in dimension three and four, which have a capacity that exceeds the PSK–limit of an AWGN channel. Nonabelian groups are of particular interest because abelian groups can generate only slepian–type signal sets having a capacity, which is upper bounded by the PSK–limit. For every convolutional code C a canonical state group S_C and a canonical transition graph B_C is introduced. The transition graph B_C corresponds to a trellis diagram, which generates the code C . It is shown that if a convolutional code is defined over a nonabelian group and if it has an abelian state group S_C then its free Hamming distance equals one.

Fredy D. Neeser:

A Simplified Derivation of the Capacity of the ISI Channel with AWGN using complex Random Variables

The 'covariance' of complex random variables can be specified by the (conventional) complex covariance and a quantity called the pseudo–covariance. Complex random variables with a vanishing pseudo–covariance are called proper. It is shown that properness is preserved under linear transformations.
The maximum–entropy theorem is generalized to the complex–multivariate case. For a given correlation matrix, the differential entropy of a random vector is maximum if and only if it is proper Gaussian with zero mean. A discrete Fourier transform correspondence between stationarity in the time–domain and uncorrelatedness in the frequency–domain is presented and used for a simplified derivation of the capacity of the N–circular channel with intersymbol interference (cf. W. Hirt and J.L. Massey, IEEE Trans. IT, vol. 34, May 1988).

Alon Orlitsky:

Interactive Communication of Balanced Distributions

(X,Y) is a pair of random variables distributed over a support set S . Person P_X knows X , Person P_Y knows Y , and both know S . Using a predetermined protocol,

they exchange binary messages in order for $P_{\mathcal{Y}}$ to learn X. $P_{\mathcal{X}}$ may or may not learn Y. The m–message complexity, $\hat{C}_m$, is the number of information bits that must be transmitted (by both persons) in the worst case if only m messages are allowed. $\hat{C}_\infty$ is the number of bits required when there is no restriction on the number of messages exchanged.

We consider a natural class of random pairs. $\hat{\mu}$ is the maximum number of X values possible with a given Y value. $\hat{\eta}$ is the maximum number of Y values possible with a given X value. The random pair (X,Y) is *balanced* if $\hat{\mu} = \hat{\eta}$. The following hold for *all* balanced random pairs. One–way communication requires at most twice the minimum number of bits: $\hat{C}_1 \leq 2\hat{C}_\infty + 1$. This bound is almost tight: for every α, there is a balanced random pair for which $\hat{C}_1 \geq 2\hat{C}_\infty - 6 \geq \alpha$. Three messages are asymptotically optimal: $\hat{C}_1 \leq \hat{C}_\infty + 3\log\hat{C}_\infty + 11$. More importantly, the number of bits required is only negligibly larger than the number needed when $P_{\mathcal{X}}$ knows Y in advance: $\hat{C}_\infty \leq \hat{C}_3 \leq \log\hat{\mu} + 3\log\log\hat{\mu} + 11$.

We apply these results to the following *correlated files* problem. X and Y are binary strings (files) within a small edit distance from each other. $P_{\mathcal{X}}$ knows X while $P_{\mathcal{Y}}$ knows Y and wants to learn X. The results above imply efficient three–message protocols for conveying X to $P_{\mathcal{Y}}$. We provide efficient one–way protocols for certain restricted cases and discuss their possible generalizations.

V.M. Blinovsky, P. Narayan, M.S. Pinsker:

AV Channel and List Decoding

An arbitrary varying channel (AV channel) without memory is described by a transition probability function $w(y|x,s)$ where $x \in X, y \in Y, s \in S$, X, Y, S are finite sets, X being an input alphabet, Y being an output alphabet and S being a channel state alphabet.

We consider transmission over an AV channel by deterministic codes of length n with fixed list decoding size L and average error probability. Let C_L be the capacity for such a transmission.

Let also C_r be the capacity of an AV channel for random codes and average error probability.

Theorem 1: $C_L \leq C_r$ and C_L is equal either 0 or C_r.

Definition: An AV channel is symmetrizable of order L, if for some distribution $p(s|x_2,\ldots,x_{L+1})$, $s \in S$, $x_2,\ldots,x_{L+1} \in X$

$$\sum_{s\in S} w(y|x_1,s)p(s|x_2,\ldots,x_{L+1}) = \sum_{s\in S} w(y|x_{\pi_1},s)p(s|x_{\pi_2},\ldots,x_{\pi_{L+1}})$$

where $\pi = (\pi_1,\ldots,\pi_{L+1})$ is an arbitrary permutation of the sequence $(1,\ldots,L+1)$.

Theorem 2: $C_L \geq 0$, if and only if an AV channel is not symmetrizable of order L. If $C_L > 0$ then $C_L = C_r$.

Theorem 3: Let $|X| = |Y| = |S| = 2$ and $C_r > 0$. Then for any AV channel there is some L such that it is not symmetrizable of order L.

Corollary: For $|X| = |Y| = |S| = 2$ we have $C_L = C_r$ for some $L < \infty$.

Marcel Rupf:

Optimum Sequence Multisets for Symbol–Synchronous Code–Division Multiple–Access Channels

The capacity region of the S–COMA channel is considered under the condition that all channel inputs fulfill the same average symbol–energy constraint. It is shown that the sum capacity is maximized by all sequence multisets which meet Welch's lower bound on the correlation of a sequence multiset. Moreover, it is also shown that the symmetric capacity in function of these sequence multisets is equal to the sum capacity, where the symmetric capacity is defined by the maximum achievable equal–rate point in the capacity region. Finally, it is concluded that S–COMA systems can use dimension or bandwidth most efficient and in a (fair) communication when the number of users is larger than or equal to the sequence length.

Paul C. Shields:

Entropy and Joint Distributions

The problem of consistent estimation of the k–th order joint distribution from observation of a finite sample path, where $k = k(n)$ is a function of path length n, is addressed. It is shown that if the process is a function of an irreducible Markov chain and $k(n) \leq (\log n)/(H + \varepsilon)$, where H is the process entropy, then the variational distance between the emprical k–block distribution and the true k–block distribution goes to 0 almost surely. A convergence in probability result also holds for the more general class of weak Bernoulli processes.

J. Simonis:

MacWilliams Identities and Coordinate Partitions

Let C be a binary linear code, with coordinate set S, and let $\mathcal{T} := \{T_1, \ldots, T_p\}$ be a partition of S in sets of size $n_u := |T_u|$. The *weight distribution of* C *with respect to* $\mathcal{T}$ is the set of numbers

$$A_{\underline{i}}(\mathcal{T}) := |\{X \in C | |X \cap T_{i_u}| = i_u \forall u\}|.$$

We show that the $A_{\underline{i}}(\mathcal{T})$ and the weight distribution $\{B_{\underline{i}}(\mathcal{T})\}$ of the dual code $C^{\perp}$ satisfy the identities

$$A_{\underline{i}} = \sum_{\underline{j}} \left(\prod_{u=1}^{p} P_{i_u}(j_u; n_u) \right) B_{\underline{j}_u}, \qquad (*)$$

where $P_i(x; \nu) := \sum_{m=0}^{\nu} (-1)^m \binom{x}{m} \binom{\nu - x}{i - m}$, the Krawtchouk polynomial of degree i. These generalized MacWilliams identities (*) can be used to prove the nonexistence of codes satisfying conditions on the minimum distance or the covering radius. Another application is a simple proof of the Assmus Mattson theorem.

Gábor Simonyi:

Trifference (jointly with János Körner)

We focus on the following two problems:
1. Trifference problem: Let $Y_{3,3}(n)$ denote the minimum length for which we can have n ternary sequences with the property that for any three of them: $\underline{x}, \underline{y}, \underline{z} \quad \exists i : \; x_i, y_i, z_i$ are three different values.

$$F_{3,3} \triangleq \liminf_{n\to\infty} \frac{Y_{3,3}(n)}{\log n} = ?$$

2. Triangle problem (asked by Vera T. Sós): Let $t(n)$ denote the minimum number of colorings of the edges of a complete graph on n vertices with three colours such that for every triangle we would have a coloring where all its edges have different colors.

$$T \triangleq \liminf_{n\to\infty} \frac{t(n)}{\log n} = ?$$

The first problem is a well–known special case of the "perfect hashing problem" the second is visibly related. We explain why they have special interest after a recent success of applying information theory in combinatorics (a result by Gargano, Körner, Vaccaro) and prove: $F_{3,3} \leq \frac{6}{\log \frac{63}{25}}$ and $\frac{1}{\log 3} \leq T \leq 1$.

Ludwig Staiger:

Information–Theoretic Aspects of Kolmogorov Complexity

Various relationships between the Kolmogorov complexity or infinite strings and measures of information content are given. The general approach taken here is to bound the complexity of a maximally complex string in a given set of strings by the Hausdorff dimension or the entropy [box dimension] of that set. It turns out that Hausdorff dimension yields lower bounds to the Kolmogorov complexity whereas under certain recursiveness constraints to the structure of the respective sets their entropy yields upper bounds.
More detailed investigations result in a generalization of two of P. Martin–Löf's theorems on the complexity of random strings to the complexity of maximally complex strings in regularly structured sets of infinite strings.

René Struik:

Covering Problems

We consider linear codes over $GF(2)$ only.
Let C be an $[n,k]R$ code with $R = \min\{r \geq 0 | d(x,C) \leq r \text{ for all } x \in \mathbf{F}_2^n\}$. A basic question is to determine the lowest dimension k s.t. an $[n,k]R$ code exists. Equivalently the problem is to determine parameters $\ell(m,r)$ with $\ell(m,r) = \min\{n | An\ [n, n-m]r \text{ code over } GF(2) \text{ exists }\}$. A trivial lower bound on $\ell(m,r)$ is $\ell(m,r) \geq \min\{n | \sum_{i=0}^{r} \binom{n}{i} \geq 2^m\}$. In the talk several improvements on known lower-bounds of $\ell(m,r)$ will be discussed and a relation with the non–linear covering problem will be given. They are based on:

- theorems in "ordinary" coding theory (mostly minimum distance bounds)
- a generalization of the concept of covering
- counting arguments

All non–existence proofs are constructive and all known bounds for $r = 2,3$ can be derived in this way.
$\ell(8,2) \geq 25(24), \ell(9,2) \geq 34(33), \ell(2m-1,2) \geq 2^m + 1 (m \geq 3)^{(2^m)}$ [Conjectured by Brualdi, Pless, Wilson],
$\ell(9,3) \geq 17(16), \ell(10,3) \geq 21(19), \ell(12,3) \geq 31(30), \ell(13,3) \geq 38(37)$ In brackets are "old" bounds.

R. Ahlswede, N. Cai and U. Tamm:

Communication Complexity of Sum–Type and Vector–Valued Functions

The communication complexity of a function F denotes the number of bits that two processors have to exchange in order to compute a function value $F(x,y)$, when initially each of the processors knows one of the arguments. The functions examined are vector–valued and sum–type function. To define the vector–valued function $V_n : \mathcal{X}^n \times \mathcal{Y}^n \to \mathcal{Z}^n$ let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be any function. $V_n((x_1,\ldots,x_n),(y_n,\ldots,y_n)) = \big(f(x_1,y_1),\ldots,f(x_n,y_n)\big)$ is obtained by componentwise evaluation of f. Accordingly, the sum–type function $S_n : \mathcal{X}^n \times \mathcal{Y}^n \to \mathbf{N}$ (or $\mathbf{Z}_p$) is defined by $S_n\big((x_1,\ldots,x_n),(y_1,\ldots,y_n)\big) = \sum_{t=1}^{n} f(x_t,y_t)$.
If, e.g., f is the logical "and", then the vector–valued function V_n can be interpreted as the intersection of the two sets represented by $(x_1,\ldots,x_n)$ and $(y_1,\ldots,y_n)$, whereas the sum–type function S_n gives the cardinality of this intersection. For both functions the communication complexity is determined. Ahlswede and Cai ([1]) show that $C(V_n) = \lceil n \log_2 3 \rceil$. $C(S_n)$ can be determined up to one bit ([4]), namely $n + \lceil \log_2(n+1) \rceil - 1 \leq C(S_n) \leq n + \lceil \log_2(n+1) \rceil$, where upper and lower bound are assumed for $n = 2^t$ and $n = 2^t - 1$, respectively.
The communication complexity of sum–type functions is considered under two different aspects. Communication stops, when a) one processor knows the result ([2]), or b) both processors know the result ([3]), ([4]). In all models, the basic algebraic tool in the proof of lower bounds is the Kronecker product in terms of which the function matrices can be expressed. The results are contained in the following papers
(Preprints 91–041, 91–053, 91–016, and 91–077, SFB 343, Universität Bielefeld)

[1] R. Ahlswede, N. Cai: On communication complexity of vector–valued functions
[2] R. Ahlswede, N. Cai: 2–way communication complexity of sum–type functions for one processor to be informed
[3] U. Tamm: On the communication complexity of sum–type functions
[4] U. Tamm: Deterministic communication complexity of the set–intersection function

A. Tietäväinen:

On Bounds for the Number of Binary Vectors with a Given Maximum Correlation

Code division multiple access (= CDMA) techniques require large families of sequences with good correlation properties. If the number of sequences is smaller than or approximately equal to the period of sequences, there are good constructions and tight bounds. On the other hand, if the number of sequences is remarkably larger than the period, there is a huge gap between bounds and constructions. This is the problem considered in this talk.

Henk van Tilborg:

Is there such a Thing as a Perfect Asymmetric–Error–Correcting Code?

For the Z–channel the following special classes are defined: 1) perfect, 2) weakly perfect, and 3) uniformly weakly perfect asymmetric–error–correcting codes (AsEC).
It turns out that the only nontrivial perfect AsEC code is the repetition code. For any weakly perfect t–AsEC code it is shown that a larger size code exists that is also t–AsEC.

Sergio Verdú:

Approximation Theory of Output Statistics (Summary)

To motivate the problem studied in this talk consider the computer simulation of stochastic systems. Usually, the objective is to compute a set of statistics of the response of the system to a given "real–world" input random process. To accomplish this, a sample path of the input random process is generated and empirical estimates of the desired output statistics are computed from the output sample path. A random number generator is used to generate the input sample path and an important question is how many random bits are required per input sample. In this work we are interested in the approximation of output statistics with arbitrary accuracy, in the sense that the distance between the finite–dimensional statistics of the true output process and the approximated output process is required to vanish asymptotically. We define the *resolvability* of a system as the number of random bits required in order to achieve arbitrary accurate approximation of the output statistics for any input process.
Although the problem of approximation of output statistics involves no codes of any sort or the transmission/reproduction of information and it deals with arbitrary (not necessarily ergodic) input statistics, we show that the resolvability of a system is equal to its Shannon capacity.

A.J. Han Vinck:

Correction of Peak–Shifts in (d,k)–sequences

We describe joint work with V.I. Levenshtein and A. Kuznetsov from Moscow. We consider codes consisting of sequences $0^{d+\alpha_1}10^{d+\alpha_2}1\ldots0^{d+\alpha_N}$, $0 \leq \alpha_i \leq k-d := q-1$. First we construct codes

$$C(w,g) = \{\underline{\alpha} \in C : \sum_{i=1}^{N} \alpha_i w_i = g(\text{mod } m), w_i \text{ and } g \text{ integer } < m\}$$

that are capable of correcting single peak–shifts of size $t = 1, 2$. We introduce the concept of perfect t–shift correcting codes and finally give a construction of systematic codes.
In the second part of the talk we show that the (linear) code defined by

$$H = \begin{bmatrix} +1 & -1 & +1 & -1 & \dots & & & & & & -1 \\ 1 & 2 & 3 & 4 & \dots & q-1 & 0 & 1 & \dots & q-2 & q-1 \\ \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \dots & & & & & & \alpha^N = 1 \end{bmatrix}, \alpha \in GF(q^r), q \geq 5$$

corrects t–shifts for $t \leq \frac{(q-1)}{2} = \frac{k-d}{2}$. The redundancy of this code is $(r+2) > \log_q(2 \cdot q^r \cdot t + 1)^2 > r + \log_q(q-1)$, which is very close to optimal.

Aaron Wyner:

Shannon Capacity of Cellular Multiaccess Channel

We begin with a short discussion of the classical Gaussian multi–access channel, and show that "TDMA" (or "FDMA") is optimal. We then discuss a simple though insightful model of the cellular multi–access channel in which neighboring cells interfere with each other. We show that, when optimal coding/decoding is used, the interference degrades performance only slightly, and sometimes even improves performance.

V.A. Zinoviev:

On Universal Families of Codes

Let $E = \{0, 1, \dots, q-1\}$. Denote by $U_i \subseteq E^n$ the block code of length n with minimal (Hamming) distance $d_i \geq 2i + 1$ and power $N_i = |U_i|$. A family of codes $U_{t_1}, \dots, U_{t_s}$, where $1 \leq t_1 < \dots < t_s \leq [(d-1)/2], d \leq [n(q-1)/q]$, we call the universal family, if for any $i, j : i \neq j$, $i, j \in \{1, \dots, s\}$, the distance $d_{i,j} = d(U_i, U_j)$ between the codes U_{t_i} and U_{t_j} satisfies the inequality $d_{i,j} \geq t_i + t_j + 1$. We give here the exact construction of the universal family of codes with asymptotically (when $n \to \infty$ and t_s is fixed) optimal parameters. The main result is the following. For any fixed integer $t \geq 1$ we construct the family of universal codes $U_1, \dots, U_t$, where $U_i, i = 1, \dots, t$, has length n , minimal distance $d_i \geq 2i + 1$ and power N_i , where

$$N_i = \frac{1}{2^{t-1}} \cdot \frac{2^n}{n^t}(1 + o(1)), \; o(1) \underset{n-\infty}{\longrightarrow} 0.$$

The power N_i of code U_i differs from the Hamming upper bound $t!2^n/n^t$ only by a multiplicative constant.

Jacob Ziv:

A Measure of Relative Entropy between two Individual Sequences with Application to Universal Classification

A new notion of empirical informational divergence (relative entropy) between two individual sequences is introduced. If the two sequences are independent realizations of two finite–order, finite alphabet, stationary Markov Processes, the empirical relative entropy converges to the relative entropy almost surely. This new empirical divergence is based on a version of the Lempel–Ziv data compression algorithm.
Applications to universal classification are discussed.

Berichterstatter: U. Tamm

Tagungsteilnehmer

Prof.Dr. Thomas Beth
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Am Fasanengarten 5, Geb. 5034

W-7500 Karlsruhe 1
GERMANY

Prof.Dr. Rudolf Ahlswede
Fakultät für Mathematik
Universität Bielefeld
Postfach 10 01 31

W-4800 Bielefeld 1
GERMANY

Prof.Dr. Richard E. Blahut
IBM Corporation
MD 0600
Route 17C

Owego , NY 13827-1298
USA

Dr. Ingo Althöfer
Fakultät für Mathematik
Universität Bielefeld
Postfach 10 01 31

W-4800 Bielefeld 1
GERMANY

Dr. Martin Bossert
AEG Mobile Communication GmbH
Abteilung Entwicklung
Wilhelm-Runge-Str. 11

W-7900 Ulm
GERMANY

Prof.Dr. Leonid A. Bassalygo
Institute for Problems of
Information Transmission
Academy of Sciences
ul. Ermolova 19

101447 Moscow GSP-4
RUSSIA

Dr. Ning Cai
Fakultät für Mathematik
Universität Bielefeld
Postfach 10 01 31

W-4800 Bielefeld 1
GERMANY

Prof.Dr. Toby Berger
Dept. of Electrical Engineering
Cornell University
392 E & TC

Ithaca , NY 14853
USA

Prof.Dr. A. Robert Calderbank
AT & T Bell Laboratories
600 Mountain Avenue

Murray Hill , NJ 07974
USA

Prof.Dr. Gerard Cohen
ENST
46, rue Barrault

F-75013 Paris

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

S-221 00 Lund

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

W-6100 Darmstadt
GERMANY

Prof.Dr. Torleiv Klöve
Institute of Informatics
University of Bergen
Hogteknologisenteret

N-5020 Bergen

Prof.Dr. Michele Elia
Dipartimento di Elettronica
Politecnico di Torino
Corso Duca degli Abruzzi, 24

I-10129 Torino

Prof.Dr. Dejan E. Lazic
Universität Karlsruhe
Forschungszentrum Informatik
Techn.Expertensysteme und Robotik
Haid-und-Neu-Strasse 10-14

W-7500 Karlsruhe 1
GERMANY

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

N-5020 Bergen

Prof.Dr. Jacobus H. van Lint
Rector Magnificus
Department of Mathematics
Eindhoven University of Techn.
Postbus 513

NL-5600 MB Eindhoven

Prof.Dr. Ingemar Ingemarsson
Dept. of Electrical Engineering
Division of Information Theory
Linköping University

S-581 83 Linköping

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

H-1364 Budapest

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

CH-8092 Zürich

Prof.Dr. Alon Orlitsky
AT&T Bell Laboratories
600 Mountain Avenue

Murray Hill , NJ 07974
USA

Prof.Dr. Herald F. Mattson
Computing Information Sciences
Syracuse University
CST 4-1116

Syracuse NY 13244-4100
USA

Prof.Dr. Mark S. Pinsker
Institute for Problems of
Information Transmission
Academy of Sciences
ul. Ermolova 19

101447 Moscow GSP-4
RUSSIA

Prof.Dr. Edward C. van der Meulen
Departement Wiskunde
Faculteit der Wetenschappen
Katholieke Universiteit Leuven
Celestijnenlaan 200 B

B-3001 Leuven

Marcel Rupf
Inst. f. Signal & Info. Processing
ISI ETF F103
ETH-Zentrum

CH-8092 Zürich

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

CH-8092 Zürich

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

Toledo , OH 43606
USA

Fredy Neeser
Inst. f. Signal & Info. Processing
ISI ETF F103
ETH-Zentrum

CH-8092 Zürich

Prof.Dr. Juriaan Simonis
Dept. of Mathematics and
Computer Science
Delft University of Technology
P. O. Box 356

NL-2600 AJ Delft

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

H-1364 Budapest

Prof.Dr. Henk C.A. van Tilborg
Department of Mathematics
Eindhoven University of Techn.
Postbus 513

NL-5600 MB Eindhoven

Prof.Dr. Ludwig Staiger
Universität-GH-Siegen
Programmiersprachen
Postfach 10 12 40

W-5900 Siegen
GERMANY

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

Princeton , NJ 08544
USA

René Struik
Department of Mathematics
Eindhoven University of Techn.
Postbus 513

NL-5600 MB Eindhoven

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

W-4300 Essen 12
GERMANY

Dr. Ulrich Tamm
Fakultät für Mathematik
Universität Bielefeld
Postfach 10 01 31

W-4800 Bielefeld 1
GERMANY

Dr. Frans M.J. Willems
Dept. of Electrical Engineering
Eindhoven University of Technology
P. O. Box 513

NL-5600 MB Eindhoven

Prof.Dr. Aimo Tietäväinen
Institute of Mathematical Sciences
University of Turku

SF-20500 Turku

Dr. Aaron D. Wyner
AT & T Bell Laboratories
600 Mountain Avenue

Murray Hill , NJ 07974-2070
USA

Prof.Dr. Victor A. Zinovjev
Institute for Problems of
Information Transmission
Academy of Sciences
ul. Ermolova 19

101447 Moscow GSP-4
RUSSIA

Prof.Dr. Jacob Ziv
ATT Bell Laboratories
2C-359
600 Mountain Avenue

Murray Hill , N.J. 07974
USA

Email - Adressen

1)	Ahlswede	sfbmath@dbiuni11
2)	Althöfer	sfbmath@dbiuni11
3)	Bassalygo	
4)	Berger	berger@ee.cornell.edu
5)	Beth	
6)	Blahut	blahut@owgvm3.vnet.ibm.com
7)	Bossert	
8)	Cai	cai@math5.mathematik.uni-bielefeld.de
9)	Calderbank	rc@research.att.com
10)	Cohen	cohen@inf.enst.fr
11)	Dorsch	
12)	Elia	elia@polito.it
13)	Helleseth	torh@ii.uib.no
14)	Ingemarsson	iz@isy.liu.se
15)	Johannesson	
16)	Klöve	
17)	Lazic	lazic@fzi.de
18)	van Lint	
19)	Marton	
20)	Massey	infort@czheth5a.bitnet
21)	Mattson	
22)	van der Meulen	
23)	Mittelholzer	
24)	Neser	
25)	Orlitsky	alon@research.att.com
26)	Pinsker	pinsker@ippi.msk.su
27)	Rupf	
28)	Shields	fax0172@4oft02.bitnet
29)	Simonis	simonis@dutiaw3.tudelft.nl
30)	Simonyi	
31)	Staiger	staiger@server.informatik.uni-siegen.de
32)	Struik	dwrs@win.tue.nl
33)	Tamm	tamm@math1.mathematik.uni-bielefeld.de
34)	Tietäväinen	tietavai@cs.utu.fi
35)	van Tilborg	wsdwhenk@urc.tue.nl
36)	Verdu	verdu@princeton.edu
37)	Vinck	mem100@de0hrz1a
38)	Willems	eleifw@urc.tue.nl
39)	Wyner	adw@research.att.com
40)	Zinoviev	zinov@ippi.msk.su
41)	Ziv	jz@ee.technion.ac.il