Math. Forschungsinstitut
Oberwolfach
E 20 102-173

MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 21/1989

Informationstheorie

14.05. bis 20.05.1989

Leitung: R. Ahlswede (Bielefeld)
J.H. van Lint (Eindhoven) und
J. Massey (ETH Zürich)

Folgende Themen standen im Vordergrund:

— Modelle für Speichern
— Algebraische Kodierungstheorie
— "Road blocks" in der Informationstheorie.

Es wurden aber auch Bezüge zur Approximationstheorie (ϵ–Entropie), Statistik (Algorithmische Beschreibung von Ensembles) und kombinatorischer Optimierung diskutiert.

Gefördert durch DFG Deutsche Forschungsgemeinschaft
© Oberwolfach

Vortragsauszüge

S. Arimoto

Information Theory and Machine Intelligence

The final goal of our research is to design a pictorial memory somewhat similar to what we humans have in brain as a human memory. Given a sequence of pictorial patterns, such a memory should be organized as a form of structured data-base which can be quickly accessed. In this talk I propose an algorithm for construction of a structured data-base in a self-organizing way when a sequence of patterns (vectors) are given and a distortion measure is defined a-priori. The data-base is constructed in a form of binary tree through comparison of the present pattern with registered patterns at tree nodes. If there exists a previously registered patterns in the tree whose distortion from the present pattern is less than a prescribed fidelty criterion $\epsilon > 0$, then the present pattern is not registered in the tree. Comparison induces a bi-partition of the pattern space and the tree yields a partition of it to various scopes of inference. Finally I point out many interesting problems remain unsolved in relation to this problem.

Th. Beth

Zero Knowledge Proofs, Secrecy and Authentication

After a short introduction to concepts of information processing the notion of secrecy is viewed simultaneously under the aspects of complexity and information theory. In this framework we present a new Zero Knowledge interactive proof system of low complexity and exponentially small residual error/cheating probability based on the DL-problem of finite groups. For the special case of multiplication in $GF(2^m)$ with normal basis representation, a very efficient algorithm is being presented.

R.E. Blahut

Channel Capacity

Some Unfinished Business Information theory was first formulated for purpose of finding the capacity of communication channels and for finding the optimum waveforms for communication. The capacity of discrete-time and continuous-time additive Gaussian noise channels was described by Shannon. Since then information theory has moved on to study many abstract problems. However, there are many problems of practical importance that have been bypassed. The purpose of this lecture is to survey the many interesting channels whose capacity is unknown. Specifically no results are known to me about the capacity of the continuous-time channel with a bandlimiter at the output (which is different from the discrete-time version of this channel). The capacity of the continuous-time channel with bandlimiter at the input is unknown. The capacity of continuous-time and discrete-time additive Gaussian noise channels with multiplicative phase noise is unknown. The capacity of doppler spread channels in unknown.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

I.F. Blake

Enumeration of Constrained Sequences

Constrained sequences, such as the (d, k) sequences, have been widely studied over the past decade. Efficient techniques to encode them, even up to their capacity, exist as well as decoding techniques that limit error propagation. They have been studied both from an information theoretic and a combinatorial point of view and this talk attempts to illuminate the relationship between the two approaches. Specifically a production rule is given that leads directly to a generating function for the maximal size catenable (d, k) sequences of length n. It is suggested that such a production rule should have an information theoretic interpretation.

A.R. Calderbank, L.H. Ozarow

Non–Equiprobable Signaling On The Gaussian Channel

Many signaling schemes for the Gaussian channel are based on finite–dimensional lattices. The signal constellation consists of all lattice points within a region $\mathcal{R}$, and the shape of this region determines the average signal power. In the limit as $N \to \infty$, the shape gain of the N–sphere over the N–cube approaches $\frac{\pi e}{6} = 1.53db$. We show that the full asymptotic shape gain can be realized in any fixed dimension by non–equiprobable signaling. The peak to average power ratio of these schemes is superior to that of equiprobable signaling schemes based on Voronoi regions of multidimensional lattices. The new shaping schemes admit a simple stage demodulation procedure.

G. Cohen

Write–Isolated Memories

A write–isolated memory (WIM) is a binary storage medium on which no change of two consecutive positions is permitted when updating. We prove that the optimal rate (zero–error capacity) for writing on a WIM is $log_2((1+\sqrt{5})/2) \simeq 0.69$. We give asymptotic group constructions achieving 0.6.

M. Cohn

Observations on Lookahead Coding for Input–Restricted Channels

Consider a discrete, lossless channel with constraints on its transitions, represented by a finite automaton. Shannon showed how to find ideal transition probabilities that allow channel capacity to be achieved. We interpret a lookahead code to be a technique which uses upcoming inputs to simulate transition probabilities which allow and encodes to attain or approach channel capacity.

We also observe that there exist channels that can be coded at capacity using lookahead alone but not state–dependence alone, and there are channels, that can be coded at capacity using state–dependence alone, but not lookahead alone.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

I. Csiszár

Arbitrarily Varying Channels as Models of Memories

Memories with some cells stuck at zero and one can be regarded as arbitrarily varying channels with three possible states (cell stuck at zero, stuck at one, or good). The capacity of AVC's, for deterministic codes with the average probability of error criterion, when the permissible state sequences are known to satisfy certain constraints but neither the encoder nor the decoder knowns the actual state sequence, has been determined by Csiszár and Narayan (1988). Applying that result to memories, when the frequencies of the two kinds of defective cells are known to be smaller than some Λ_0 and Λ_1, the storage capacity (under the average probability of error criterion) turns out to be positive iff $\sqrt{\Lambda_0}+\sqrt{\Lambda_1} < 1$. An explicit capacity formula is also available but it is tedious.

The results reported in this paper were obtained partly with P. Narayan and partly with the student B.V. Than.

S.M. Dodunekov

Optimal Linear Codes

Let $F_q = GF(q)$ be a finite field with q elements and let F_q^n be an n–dimensional vector space over F_q. A space $C \subseteq F_q^n$ is called to be an $[n,k,d]$ =[length, dimension, minimum distance]–code, if

$$K = \dim_{F_q} C, \quad d = \min_{\substack{x,y \in C \\ x \neq y}} d(x,y)$$

($d(x,y)$ is the Hamming distance). n, k, d are so–called basic parameters of a code.

One of the main problems of the constructive coding theory is the following : given two basic parameters to optimize the third. More precisely, let us consider the following three functions:

$$N_q(k,d) = min\ n, \exists \quad [n,k,d] - code;$$
$$K_q(n,d) = max\ k, \exists \quad [n,k,d] - code;$$
$$D_q(n,k) = max\ d, \exists \quad [n,k,d] - code.$$

Codes with parameters

$$[N_q(k,d),k,d],\ [n,K_q(n,d),d],\ [n,k,D_q(n,k)]$$

are said to be optimal.

A survey of some problems and recent results concerning optimal linear codes is presented.

B. Dorsch

Algebraic Maximum Likelihood Decoding of Some Classes of Blockcodes

The performance of algebraic blockcodes is limited mainly by Bounded Minimum Distance Decoding (BMD), where only up to $t = \lfloor (d_0+1)/2 \rfloor$ errors can be corrected, d_0 =designed– or BCH–minimim–distance. Correcting $t+1$ or $t+2$ errors as in some known algorithms doesn't increase the performance much. Egon Schulz describes (in this Dr.–thesis 1988 at

Gefördert durch DFG Deutsche Forschungsgemeinschaft

Techn. Hochschule Darmstadt) a new algorithm to decode algebraically much more than t errors, for some classes even up to any number (Maximum Likelihood Decoding MLD). The algorithm with MLD can be used especially for such codes of length n, dimension k, with elements from $GF(q)$, for which each codeword is determined by a single element $u \in GF(q^k)$ in a transform domain, as it is the case for some BCH–codes and the powerful class of QR–codes (usually with minimum distance D much greater than d_0). A new improved estimate of block error probability P_e for a BCH is derived and compared to simulation results, showing that for AWGN (with antipodal signaling and coherent demodulation) a signal/noise–ratio $E_b/N_0 \approx 2,5dB$ can be achieved by MLD (compared to $\gtrsim 5,5dB$ with BMD) with binary codes, $n \approx 1000,\ k \approx 250$.

G. Dueck

Combinatorial Optimization in Information Theory

Two new optimization heuristics are presented for discrete optimization: Threshold Accepting algorithms (TA) and the Great Deluge Algorithm (GDA). In this structure they resemble the well–known Simulated Annealing approach (SA), but they operate with different acceptance rules for worse intermediate configurations. Many empirical results show that TA and GDA perform much better than the classical SA method. In information theory, SA was already used to construct new error–correcting codes. We show results with TA and GDA. Another interesting problem is to compute capacity regions for various (multi–user) communication systems. These computations were very difficult in the past, even for small examples. TA and GDA, however, can be used to compute those complicated formulas very fast. A main advantage of the new methods lies in their extremely simple structure. Real implementations of those methods in FORTRAN, say, can be mostly written using only up to one hundred lines of code.

I.I. Dumer

Nonbinary Codes with Distance 4; 5 and 6, asymptotically exceeding BCH–Codes

We construct linear code C_d, $d = 4;5;6$, over arbitrary alphabet $L = GF(q)$, which has asymptotical redundancy $\sim 1.5\ log_q n$, $\sim 2.4\ log_q n$ and $\sim 3\ log_q n$ parity check symbols respectively instead of $\sim 2\ log_q n$, $\sim 3\ log_q n$ and $\sim 4\ log_q n$ symbols for BCH–codes with length $n \to \infty$. The decoding is also less complex than BCH–decoding and requires $\sim 2.4n\ log_q n$ additions and $\sim 2.4n\ log_q n$ multiplications in L for $d = 5$.

The code C_d is constructed by parity check matrix

$$H(s, X, j_1, \dots, j_{d-1}) = \begin{Vmatrix} x_1^{j_1} & \dots & x_n^{j_1} \\ \vdots & \dots & \vdots \\ x_1^{j_{d-1}} & \dots & x_n^{j_{d-1}} \end{Vmatrix}$$

with locator set $X = \{x_1, \dots, x_n\} \subset L^s$ and $d-1$ numbers $j_1 = q^t + 1, \dots, j_{d-1} = q^{t+d-2} + 1$.

Theorem 1 C_d has distance $d \geq 4$, iff: a) all locators are not proportional over L (i.e. $x_i \neq \xi x_j$ for $\forall i, j,\ i \neq j$ and $\forall \xi \in L$.). Codes C_5 and C_6 have distance 5 and 6 respectively

Gefördert durch DFG Deutsche Forschungsgemeinschaft

iff two conditions hold: condition a) and condition b) each two–dimensional L–subspace in L^s (L–plane) intersects with locator set X in 3 or less points.

We obtain minimal redundancy by choosing s and t as: $s = 2m,\ t = m-1$ for $d = 4$; $s = 2m+1,\ t = m-1$ for $d = 5$; $s = 2m,\ t = m-2$ for $d = 6$. We use the set of $(q^s-1)/(q-1)$ nonproportional locators in C_4. The set X, constructed in C_5 and C_6, is a cubic manifold in $L^{6\ell+1}$ (i.e. $s = 6\ell+1$), generated by locators $x = (\tau_0, \tau_1, \dots, \tau_{s\ell})$ with:

$$\tau_0 = 1,\ \tau_{6i} = N_2(\tau_{6i-5}, \tau_{6i-4} + N_3(\tau_{6i-3}, \tau_{6i-2}, \tau_{6i-1}),\ i = 1, \dots, \ell,$$

where $N_2(\alpha, \beta)$ and $N_3(d, \beta, \gamma)$–the norms of elements in L^2 and L^3 respectively as functions of their coordinates.

Theorem 2 Conditions a) and b) hold for locator set X with $|X| = q^{5\ell}$.

A. Dür

On the Decoding of Doubly–Extended Reed–Solomon Codes

In my talk I have presented a new bounded–distance decoding algorithm for doubly–extended Reed–Solomon codes. This algorithm is based on Berlekamp's algorithm for decoding Reed–Solomon codes and always produces a candidate for the error–locator polynomial of degree less than or equal to the packing radius of the code. Stated in terms of shift registers, the algorithm solves the following problem:

Given a sequence $s_0, s_1, \dots, s_x$ in K, find the longest subsequence $s_L, s_{L+1}, \dots, s_M$ that can be generated by a linear recursion from the subsequence $s_0, s_1, \dots, s_{L-1}$, and the generating recursion.

Furthermore, I have shown that the covering radius of a doubly–extended Reed–Solomon code of minimum distance d is either $d-2$ or $d-1$, and I have determined the exact value unless $q/2 + 3 < d < q$.

M. Elia

Symmetric Functions over Finite Fields

A basic problem concerning symmetric functions is: Given a convenient set of power symmetric functions $S_{\ell_i} = \sum_{j=1}^{t} x_j^{\ell_i},\ i = 1, \dots, t$, to compute the elementary symmetric functions $\sigma_h = \sum x_1 \dots x_h,\ h = 1, \dots, t$ and the sum is over all possible permutations of the variables. The decoding of linear cyclic codes up to the error correction capabilities is an instance of this problem. The Berlekamp–Massey algorithm computes $\sigma_1, \sigma_2, \dots, \sigma_t$ from $S_1, S_3, \dots, S_{2t+1}$ and then provides the decoding of BCH codes within the BCH–bound.

Here we obtain the solution of the symmetric function problem for $\sigma_1, \sigma_2, \sigma_3$ and σ_4 given S_1, S_{-1}, S_3, S_{-3} and therefore we define the class of 4–errors correcting code $(2^m+1, 2^m+1-2m, 9)$, m even. Algebraic decoding procedures for $(33, 13, w)$, $(33, 11, 11)$ and $(47, 24, 11)$ codes are also shown, therefore completing the analysis by Bours, Taussen,

Gefördert durch DFG Deutsche Forschungsgemeinschaft

van Aspeidt and van Tilborg concerning the algebraic decoding of every cyclic code with $n \leq 51$.

Th. Ericson

Generalizations of the Johnson and the Bassalygo–Elias Bounds

Theorem 1 (Johnson bound): Let T be the size of a code with constant composition P and minimum distance d. The distance function is such that $\psi(P) \triangleq \sum_{a,b} P(a)P(b)d(a,b)$ is concave. Then $T \leq \frac{d}{d - n\psi(P)}$; $n\psi(P) < d$, where n is the length of the code.

Theorem 2 (Bassalygo–Elias bound): Suppose the alphabet has a group structure and let the distance function have the form $d(a,b) = w(a-b)$. Denote by $A_n(d)$ the maximal size of a d–code and let $T_n(P,d)$ denote the same quantity under the additional condition that all codewords have the same composition P. Define

$$B_n(P) = \frac{n!}{\prod_{a \in X} [nP(a)]!}$$

(provided all quantities $nP(a)$ are integers) when X denotes the alphabet. The following inequality holds:

$$A_n(d) \leq \frac{|X^n|}{B_n(P)} T_n(P,d)$$

$P \in \mathcal{P}(X)$ is arbitrary.

L. Bassalygo, S. Gelfand, M. Pinsker

Coding for Channels with Localized Errors

The notion of a code for the binary channel with $\leq t$ localized errors is introduced as follows.

A configuration E is a subset in $\{1, \ldots, n\}$. Denote by $\mathcal{E}_t$ the set of all configurations with $\#(E) \leq t$. A code for channel with $\leq t$ localized errors of length n and size M is a pair (φ, ψ) where $\varphi : \{1, \ldots, M\} \times \mathcal{E}_t \to \{0,1\}^n$ is an encoding mapping and $\varphi : \{0,1\}^n \to \{1, \ldots, M\}$ is a decoding mapping. A code is said to correct all localized errors of multiplicity $\leq t$ iff $\psi(\varphi(m,E) \oplus e) = m$ for all $m \in \{1, \ldots, M\}$, all $E \in \mathcal{E}_t$ and all error vectors $e = (e_1, \ldots, e_n) \in \{0,1\}^n$ such that $e_i = 0$ for $i \notin E$; here $\oplus$ is the mod 2 summation of binary vectors.

Theorem 1 For any code correcting all localized errors of multiplicity $\leq t$ we have

$$M \leq 2^n / \sum_{i=0}^{t} \binom{n}{i}.$$

Theorem 2 There exists a code correcting all localized errors of multiplicity $\leq t$ such that

$$M \geq \frac{1}{2n} \left[2^n / \sum_{i=0}^{n} \binom{n}{i}\right].$$

Gefördert durch DFG Deutsche Forschungsgemeinschaft

Corollary. The asymptotic ($n \to \infty$) rate $R(\tau)$ of an optimal code correcting $\leq t = \tau n$ localized errors (τ fixed) is given by

$$R(\tau) = 1 - h(\tau)$$

where h is the binary entropy function.

Ch. Heegard

Limits on Coding for Computer Memory

The role of error correcting codes in the design of semiconductor random access memory systems (RAM's) is twofold: (1) the problem of reliable storage (i.e., the control of random errors in the operation of the memory) and (2) the problem of yield (i.e., the control of defects in the manufacturing process). This talk concerns the latter.

In practice, when a large array of memory cells is constructed, it is often the case that many of the individual cells are defective. To improve on the yield (i.e., the fraction of acceptable memory arrays) spare rows and columns are constructed and used to replace rows and columns that are found to be defective (i.e., contain defective cells). For any fixed rate, $R > 0$, ($R = M/N$, M = information size of memory, $N = M + X$, X =number of spare cells) and defect density, p, (fraction of defective cells) there is a critical size, $M^*(R, p)$, for which the yield is small whenever a memory of size $M > M^*$ is constructed. A study of $M^*(R, p)$ shows row/column replacement is: (1) very effective for small p and large rate $R < 1$, $R \approx 1$ and (2) dramatic improvements are not found for smaller R. In the case of smaller R (for a fixed p, R smaller makes M^* larger) error–correcting codes (e.g. a single error–correcting Hamming code) in conjunction with row/column replacement is a much more effective method of improving yield.

T. Helleseth

Legendre Sums and Codes related to QR codes

This talk will give connections between Legendre sums and the weights of the codewords in some circulant codes which are related to QR codes.

Let $F = GF(p)$ be a finite field with p elements and let $\left(\frac{x}{p}\right)$ denote the Legendre symbol. Let C denote the binary circulant code of length p whose top row equals $\mathbf{a} = (a_i)$ where $a_i = 1$ iff i is a square (mod p) and $a_i = 0$ otherwise. Then the weight of the codeword in C which is the sum of the rows $j_1, \ldots, j_r$ can be expressed in terms of the Legendre sum

$$w = \frac{1}{2}\left(p + (-1)^{r-1}\left(\sum_{t \in F}\left(\frac{f(t)}{p}\right) - \sum_{k=1}^{r}\left(\frac{g_k(j_k)}{p}\right)\right)\right)$$

where $f(t) = \prod_{i=1}^{r}(t - j_i)$ and $g_k(t) = \dfrac{f(t)}{t - j_k}$.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

The results are proved using methods for solving system of equations in finite fields and by using Gaussian sums. Generalizations of the above results are also discussed.

R. Johannesson, K.Sh. Zigangirov

A Lower Bound on the Distance Profile for fixed Convolutional Codes

It is well–known that a good computational performance for sequential coding of a convolutional code requires a rapid initial growth of the column distances. This led to the introduction of the $(m+1)-$ tuple $\underline{d} = [d_0, d_1, \ldots, d_m]$, which is called the distance profile. d_j, $0 \leq j \leq m$, is the j–th order column distance and m is the memory of the code. In the talk we show that there exists a fix, binary convolutional code of rate $R = b/c$ and memory m whose column distances satisfy

$$d_j \geq \rho c(j+1)$$

in $0 \leq j \leq m$, where ρ is the Gilbert–Varshamov parameter, i.e. the solution of $h(\rho) = 1-R$.

T. Kløve

Disjoint Distinct Difference Sets

An (I,J)–set of Disjoint Distinct Difference sets (DDD) is a set $\Delta = \{\Delta_1, \Delta_2, \ldots, \Delta_I\}$ where $\Delta_i = \{a_{ij} | 1 \leq j \leq J\}$ for $1 \leq i \leq I$ are disjoint sets of positive integers such that for each i, all the differences $a_{ij} - a_{ij'}$ with $j \neq j'$ are distinct. Usually we assume that the elements of Δ_i are sorted in increasing order, i.e. $1 \leq a_{i1} < a_{i2} < \cdots < a_{iJ}$. Let

$$h = h(\Delta) = \max \{a_{ij} \,|1 \leq i \leq I,\ 1 \leq j \leq J\},$$
$$H(I,J) = \min \{h(\Delta) \mid \Delta \text{ is an } (I,J) - DDD\}$$

It is known that $H(1,J) \geq J^2 - 2J^{\frac{3}{2}}$.
Clearly $H(I,J) - 1 \geq H(I-1,J)$. Hence we have

- $H(I,J) \geq H(1,J) + I - 1.$

Counting the total number of elements we get

- $H(I,J) \geq I \cdot J.$

For example for $J = 3$ we have $H(I,3) = 3I$ for $I \geq 2$ as is shown by the following construction:

$$\Delta_i = \{i, I+i, 2I+1+i\} \quad \text{for } 1 \leq i \leq I$$
$$\Delta_I = \{I, 2I, 2I+1\}.$$

In general we have a similar result:
Let $a_1, a_2, \ldots, a_J$ be a sequence which satisfies the following condition:

(*) if $|(j-k)-(r-s)| \leq 1, j > k$ and $a_j - a_k = a_r - a_s$ then $j = r$ and $k = s$.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

Let $I > I_0 = \max\{(a_j - a_k) - (a_r - a_s) \mid |(j-k)-(r-s)| \leq 1\}$ and define $\Delta = \{\{a_{ij} | 1 \leq j \leq J\} \mid 1 \leq i \leq I\}$ by

$$a_{ij} \equiv a_j + i \text{ (mod I)}\ ,\ (j-1)I < a_{ij} \leq jI.$$

Then Δ is a DDD and $h(\Delta) = IJ$. In particular $H(I,J) = IJ$ for $I > I_0$.
Sequences satisfying (*) may be constructed as follows: Let a, b, c be integers such that $a \not\equiv b \text{ (mod 2)}$ and $gcd(a,p) = 1$ where p is an odd prime, $p \geq J-1$.
Define a_j by

$$a_j \equiv aj^2 + bj + c \text{ (mod 2p)}\ ,\ 0 \leq a_j < 2_p.$$

Combining these results we get

$$L(J) \lesssim 4J$$

where $L(J)$ is minimal such that $H(I,J) = IJ$ for all $I \geq L(J)$.
Since $H(I,J) \geq J^2 - 2J^{\frac{3}{2}} + I - 1$ we get $L(J) \gtrsim J$.

Kingo Kobayashi

Marginal Processes of jointly Markov Process.

To probe the essential character in the coding for Markov source, we study the marginal processes $\{X_n\}$ and $\{Y_n\}$ of jointly Markov process $\{X_n, Y_n\}$. In general, these marginal processes are not necessarily Markovian. Here we establish a theorem which gives a sufficient condition for a function process of Markov chain (so called sofic system) being Markovian.
Let $M = [m_{ij} : i,j \in S] = [M_{ab} : a,b \in \mathcal{X}]$ be the transition matrix of a Markov chain with the output alphabet $\mathcal{X}$ and the set of internal state S, where submatrices M_{ab} correspond to the output assignment φ of states.
Then we have

Theorem. If for any $a,b,c \in \mathcal{X}$ it holds that

$$M_{ab}M_{bc}\underline{1} = M_{ab}\underline{1} \cdot \frac{u_b}{u_b \cdot \underline{1}} M_{bc}\underline{1}, \qquad \circledast$$

then $\{X_n = \varphi(S_n)\}$ is Markovian, where $\underline{u} = \{\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_\alpha\}$ is the stationary distribution of M and $\underline{1} = (1, \ldots, 1)'$.
Under some weak condition, the condition $\circledast$ is also necessary.

J. Körner

A Common Framework for Zero–Error Problems in Information Theory.

Let $\mathcal{F}$ and $\mathcal{G}$ be two families of graphs on the same vertex set. We say that $\mathcal{F}$ is covered by $\mathcal{G}$ if $\forall F \in \mathcal{F}\ \ \exists G \in \mathcal{G}$ with $E(F) \subset E(G)$, where $E(F)$ is the edge set of F. Let $t(\mathcal{G}, \mathcal{F})$ denote the cardinality of the smallest subfamily $G' \subset \mathcal{G}$ for which $\mathcal{G}'$ covers $\mathcal{F}$. Many problems in information theory can be formulated in this language.
Let K_n denote the complete graph on n vertices and let $\mathcal{F}_{k,n}$ be the family of all the subgraphs of K_n on k vertices (with isolated points added). For a graph G with $|V(G)| <$

Gefördert durch DFG Deutsche Forschungsgemeinschaft

n the graph G' is an n–spread of G if $|V(G')| = n$ and $\exists \quad f : V(G') \to V(G)$ with $(a,b) \in E(G') \Leftrightarrow (f(a), f(b)) \in E(G)$.
Examples:

1) Shannon capacity of graph G
   $\mathcal{F} = \mathcal{F}_{2,n}$ $\mathcal{G}$: all the n–spreads of G.
2) Perfect hashing=zero–error capacity for list codes
   $\mathcal{F} = \mathcal{F}_{k,n}$
   $\mathcal{G}$: all the n–spreads of G, especially for (b,k)–hashing: $G = K_b$.
3) (i,j)–separating systems
   $\mathcal{F}$: all the bipartite graphs with color classes of i resp. j vertices
   $\mathcal{G}$: all the n–spreads of K_2
4) qualitatively k–independent b–partitions
   $\mathcal{F}$: all the bipartite graphs on k vertices
   $\mathcal{G}$: all the n–spreads of K_b.

Sub–additive functionals give non–existence bounds working reasonably in cases 1 and 2. Limitations and merits of the technique are discussed.

K.–U. Koschnick

Coding for Write Unidirectional Memories

Write Unidirectional Memories ($WUM's$) have been introduced by Borden and Willems/ Vinck. They are binary storage devices having the constraint that when updating the information stored by a WUM the encoder can write $1's$ to some positions of the WUM or $0's$ to some position of the WUM but is not permitted to write combinations of $0's$ and $1's$.

$WUM's$ have been studied intensively by several authors. Some basic results are obtained. The optimal rate of a WUM–code is known to be $\log_2 \frac{\sqrt{5}+1}{2} \approx 0.694$. The best known WUM–code has been constructed by Zhang and has the rate $\log_2 307/15 \approx 0.5508$.

An important subclass of WUM–codes is the class of (n,k)–homogeneous WUM–codes. A homogeneous WUM–code consists solely of permutations of a small number of basic sets with a certain property. All known good WUM–codes are of this type.

Using Zhang's method of building basic WUM sets by combining so called WUM patterns and by using some new ideas for solving the task of finding disjoint permutations of these basic sets we have constructed two new WUM–codes. The rates of these codes are 0.5525 resp. 0.5637.

A.V. Kuznetsov

Defective Channels and Defective Memories

The general defective channel (GDC) is defined as a finite set of arbitrary deterministic mappings φ_s, $s \in S$. It is supposed that the mapping φ_s is realized by some physical channel when it is used for the transmission of some message and has a state $s \in S$. We consider the case when the encoder knows, but the decoder does not know the mapping φ_s which will be realized by the physical channel during the transmission of the message.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

The capacity of such GDC is determined by the cardinality $|Y_s|$ of the set of symbols available at the output of the channel when it is in the worst state s, e.g. $|Y_s|$ is minimum. From such information–theoretical point of view Write Once Memories ($WOM's$), Write Unidirectional Memories ($WUM's$) and some other $W\_M's$ can be considered as GDC. This allows us to estimate the capacity of $WOM's, WUM's, \ldots$. The examples are given. The GDC with error is considered as well.

H. Marko

The Controlled Information Source

The bidirectional communication theory, published 1966 in German and 1973 in the IEEE Trans. of Com. in English, uses the controlled information source which produces the present symbol x according to the conditional probability $p(x|x_n y_n)$. Here x_n denotes n past symbols of the own sequence and y_n n past symbols of the controlling sequence. Two entropies are given by:

$$H(x) = \lim_{n\to\infty} E[-\log p(x|x_n)] \text{ as usual, and}$$
$$F(x) = \lim_{n\to\infty} E[-\log p(x|x_n y_n)] \leq H(x), \text{ called "free entropy".}$$

The directed transinformation $y \to x$ is defined as:

(1) $T(x|y) = H(x) - F(x) \geq 0$.

For a bidirectional communication (dialogue) two theorems hold:

(2) $T(x|y) + T(y|x) = T_{\text{Shannon}}$

(3) $\sigma_x + \sigma_y \leq 1$, where $\sigma_x = \dfrac{T(x|y)}{H(x)}$ and $\sigma_y = \dfrac{T(y|x)}{H(y)}$ are the stochastic coupling coefficients.

A coding theorem states that the channel capacity needed to transmit all information in both directions is:

(4) $\left.\begin{array}{l} C_{x\to y} = F(x) + \varepsilon < H(x) \\ C_{y\to x} = F(y) + \varepsilon < H(y) \end{array}\right\}$ for noiseless and delayless channels with priority to fulfill the real–time condition.

The evolution of $p(x|x_n y_n)$ via a learning process (conditioning) leads to the understanding of the semantics or pragmatics of information. Biological examples are given. Possible extentions and unsolved problems are mentioned.

J. L. Massey

Causality, Stochastic Dependence, and Directed Information

A discrete channel is a specification of $P(y_n|x^n y^{n-1})$ for all $n \geq 1$ and is memoryless if $P(y_n|x^n y^{n-1}) = P(y_n|x_n)$, $\forall n$. The directed information from the input sequence X^N to the output sequence Y^N is defined (closely following an idea of Marko published 20 years ago) as

$$I(X^N \to Y^N) = \sum_{n=1}^{N} I(X^n; Y_n|Y^{n-1}).$$

Gefördert durch DFG Deutsche Forschungsgemeinschaft

The following properties are proved:

(1) For a discrete channel used without feedback, $P(y^N|x^N) = \prod_{n=1}^{N} P(y_n|x^n y^{n-1})$, where no feedback means $P(x_n|x^{n-1}y^{n-1}) = P(x_n|x^{n-1})$, $\forall n$.

(2) $I(X^N \to Y^N) \leq I(X^N;Y^N)$ with equality if the discrete channel is used without feedback.

(3) For a discrete memoryless channel, $I(X^N \to Y^N) \leq \sum_{n=1}^{N} I(X_n;Y_n)$ with equality if and only if $Y_1, Y_2, \ldots, Y_N$ are independent.

Define now a causal system of discrete channels and sources to mean $P(y_n|x^n y^{n-1}u^k) = P(y_n|x^n y^{n-1})$ for every channel and every source U^k, $\forall n$, $\forall k$.

(4) In a causal system, $I(U^K;Y^N) \leq I(X^N \to Y^N)$.

Properties (3) and (4) give a simple proof of the well–known fact that the capacity of a discrete memoryless channel is not increased by feedback.

E.C. van der Meulen, K.U. Leuven

Matching and Coding Results in Multi–User Communication

(1) Matching results (joint with S. Gelfand, IPIT, Moscow). Necessary and sufficient conditions are derived for the reliable transmission of a two–component source over a multi–user channel in two situations: (i) for the transmission of an arbitrarily correlated two–component source over a capability–degraded broadcast channel, and (ii) for the transmission of a conditionally independent two–component source over an arbitrary discrete memoryless multiple–access channel. Specifically, we have found

Theorem 1: An arbitrarily correlated source $\{S, P(s,t), T\}$ can be reliably transmitted over a d.m. capability–degraded BC $\{\mathcal{X}, P(y,z|x), \mathcal{Y} \times \mathcal{Z}\}$ if and only if

$$\begin{aligned} H(S,T) &\leq \min\{I(X;Y), I(X;Y|U) + I(U;Z)\} \\ H(T) &\leq I(U;Z) \end{aligned}$$

for some probability distribution of the form $P(u,x,y,z) = P(u)P(x|u)P(z|x,y)$.

Theorem 2: A correlated two–component source $\{S, P(s,t), T\}$ such that S and T are conditionally independent given K can be reliably transmitted over a d.m. MAC $\{\mathcal{X} \times \mathcal{Y}, P(z|x,y), \mathcal{Z}\}$ if and only if

$$\begin{aligned} H(S|T) &\leq I(X;Z|Y,T,\varphi) \\ H(T|S) &\leq I(Y;Z|X,S,\varphi) \\ H(S,T|K) &\leq I(X,Y;Z|K,\varphi) \\ H(S,T) &\leq I(X,Y;Z) \end{aligned}$$

for some probability distribution of the form

$$P(q,s,t,x,y,z) = P(q)P(s,t)P(x|s,q)P(y|t,q)P(z|x,y).$$

(2) Coding results (joint with R. Vanroose, K.U. Leuven, Belgium). Vanroose (IEEE IT, Sept. 1988) investigated the binary switching multiple–access channel and established its zero–error capacity region. It turns out that uniquely decodable codes for the BSMAC can

Gefördert durch DFG Deutsche Forschungsgemeinschaft

be carried over to obtain UD code pairs for the Blackwell broadcast channel for every rate pair in the capacity region of the Blackwell BC. This method yields consistently higher rate pairs than the codes for memories with defects (due to Kuznetsov and Tsybakov (1974)) originally used by Gelfand to establish the capacity region of the Blackwell BC.

P. Narayan, I. Csiszár

The Gaussian Arbitrarily Varying Channel

The Gaussian arbitrarily varying channel (AVC) with input constraint Γ and state constraint Λ admits input sequences $\underline{x} = (x, \ldots, x_n)$ of real numbers satisfying $\frac{1}{n}\sum_{i=1}^{n} x_i^2 \leq \Gamma$, $\Gamma > 0$, and state sequences $\underline{s} = (s_1, \ldots, s_n)$ of real numbers satisfying $\frac{1}{n}\sum_{i=1}^{n} s_i^2 \leq \Lambda$, $\Lambda > 0$; the output of the channel is $\underline{x} + \underline{s} + \underline{V}$, where $\underline{V} = (V_1, \ldots, V_n)$ is a sequence of independent and identically distributed Gaussian random variables with mean 0 and variance σ^2. It is shown that the capacity of the Gaussian AVC for deterministic codes and the average probability of error criterion is $\frac{1}{2}\log\left(1 + \frac{\Gamma}{\Lambda + \sigma^2}\right)$ if $\Gamma > \Lambda$, and is 0 if $\Gamma \leq \Lambda$.

H. Noltemeier

Voronoi Trees

A new data structure — Voronoi trees VT — are introduced which allows the comprehensive representation of proximity properties of finite sets of an arbitrary quasi–metric space.

Some properties are deduced, furthermore experimental results are reported and some fields of applications are pointed out.

M.S. Pinsker

On ε–Entropy

We consider epsilon entropy and epsilon entropy rate for several classes for deterministic arbitrarily varying sources.

The formula is given for epsilon entropy rate $\overline{H}_\varepsilon(\sigma)$ of a set of functions which is the response of linear time invariant filter with the square criterion:

$$\overline{H}_\varepsilon(\sigma) \triangleq \lim_{T\to\infty} T^{-1} H_\varepsilon(\Sigma_T),$$

here $H_\varepsilon(\Sigma_T)$ is the epsilon entropy of the class Σ_T of functions which can be represented in the form

$$f(t) = \int_{-\frac{T}{2}}^{\frac{T}{2}} \varphi(\tau)\sigma(t-\tau)d\tau, \quad \int_{-\frac{T}{2}}^{\frac{T}{2}} \varphi^2(t)dt \leq PT,$$

Gefördert durch DFG Deutsche Forschungsgemeinschaft

$\sigma(t) \in L_2(-\infty, \infty)$ is given function and P is fixed positive number. Also we give expression for epsilon–entropy of the class function

$$\sum \triangleq \{f(t) : \int_{-\frac{1}{2}}^{\frac{1}{2}} (f^{(k)}(t))^2 dt\}, \qquad f(t) \in L_2(-\frac{1}{2}, \frac{1}{2}), \quad f(\frac{1}{2}) = 0.$$

J.P.M. Schalkwijk

The 0.63056–Road Block

We consider equal rate $R = R_1 = R_2$ transmission over the binary multiplying channel (BMC). Shannon derived a lower and upper bound of 0.61695 and 0.69424, respectively, for the rate R in bit per transmission. Schalkwijk gave a simple coding strategy that yields $R =$ 0.61914 in excess of Shannon's inner bound 0.61695. By a technique called bootstrapping the author later improved on his original strategy now obtaining $R = 0.63056$. Zhen Zhang, et al., and Hekstra, et al. lowered Shannon's outer bound to, respectively, 0.64891 and 0.64628. It appears that the remaining discrepancy between 0.63056 and 0.64628 can only be resolved by studying the so called Shannon strategies in detail. In this paper we make a start with such a study using the author's unit square representation of these strategies.

G. Simonyi

Restricted Memories with Uninformed Encoder

Different types of restricted memories were widely investigated in the last few years. We give a short summary about the lack of knowledge in those cases when the encoder does not know the previous state of the memory. Two conjectures in extremal set theory related to WUM's (write–undirectional memories) will be presented.

Recently Ahlswede, Cai and Zhang introduced new extremal problems for graphs some of which can be interpreted as "memory problems" with uninformed decoder and informed encoder. We introduce an analogous problem with uninformed encoder.

H. Stichtenoth

Good Codes from Algebraic Geometry

Goppa's algebraic geometric codes have been used by Tsfasman, Vladuts and Zink (and others) for the construction of asymptotically good families of codes over $\mathbf{F}_q$, using deep results from algebraic geometry. On the other hand, special curves (or algebraic function fields) yield some classes of good codes of "finite" length: the rational function field $\mathbf{F}_q(z)$ yields RS–codes (resp. their generalizations) of length $\leq q+1$, the Hermitian function field $y^{\sqrt{q}} - y = x^{\sqrt{q}+1}$ yields good codes of length $\approx q \cdot \sqrt{q}$. We present a new function field $y^q + y = x^{q_0}(x^q + x)$, $q = 2q_0^2$ (joint work with J.P. Hansen, Aarhus). It has the maximal number of rational points of a field of genus $g = q_0(q-1)$ (but less than the Hasse–Weil bound $q + 1 + 2g\sqrt{q}$), and the resulting codes have length q^2 and very good parameters,

Gefördert durch DFG Deutsche Forschungsgemeinschaft ©

e.g. for $q = 32$ we obtain $[1024, k, d]$–codes with $k + d \geq 901$ for any k. The codes can be described explicitly, and there is a good decoding algorithm (found by T. Høholdt).

A. Tietäväinen

Covering Radius Problems and Character Sums

Using a modification of the Delsarte–MacWilliams approach we get an upper bound for the covering radius R of a binary code of length n and with dual distance d' in the following form.

Theorem $R < \frac{n}{2} - (\sqrt{u} - \sqrt[6]{u})\sqrt{n-u}$ where $u = \left\lfloor \frac{d'-2}{2} \right\rfloor$.

For small values of d' a power sum method gives better results.

B.S. Tsybakov

Randomized and Unrandomized Multiple Access Algorithms

We consider packet–data networks with multiple access algorithms (MAA). We define a concept of randomized MAA (RMAA). A special case of RMAA for which probability of packet transmission in a slot can be only 0 or 1 is called by unrandomized MAA (URMAA).

Well known examples of RMAA are ALOHA and STACK MAA's. Well known example of URMAA is part–and–try MAA.

We ask "Is it possible to get more efficient data transmission in the network using RMAA instead of URMAA in sense of network throughput or in sense of mean packet delay?"

The answer is positive in general case. There are simple examples of non–Poisson input traffic for which network has zero throughput for every URMAA and non–zero for some RMAA.

The answer is negative when input traffic is Poisson. We prove even more. Namely for each RMAA there exists a URMAA equivalent to the RMAA in sense of properly defined mutual distribution of channel and packet histories. We do not only prove the equivalence but also construct equivalent URMAA for every given RMAA. For example we represent ALOHA and STACK RMAA in URMAA form.

Main results of the paper were published in "Problems of Information Transmission" vol. 25, N 1, 1989.

F. Willems

A Partitioning Lemma and its Applications

Suppose we have a 0-1-matrix with M_1 rows, M_2 columns and with E ones. Then the index–sets $\{1, \ldots, M_1\}$ and $\{1, \ldots, M_2\}$ can be partitioned into $M_1/2$ resp. $M_2/2$ 2–element cells such that the number of product–cells with 4 ones does not exceed $E(E-1)/2(M_1-1)(M_2-1)$. This can be proved simply by random partitioning. Using this result we can give a direct and simple proof of the fact that for the broadcast channel the average–error capacity

Gefördert durch DFG Deutsche Forschungsgemeinschaft

region and the maximal-error capacity region are identical. Under certain conditions the result could be used to obtain a good memory from a (larger) bad one.

A.D. Wyner, J. Ziv

Some Asymptotic Properties of the Entropy of a Stationary Ergodic Data Source with Applications to Data Compression

In this talk we will obtain theorems concerning the entropy of a stationary ergodic information source, and use these results to yield some insight into the workings of certain data-compression coding schemes, in particular the Lempel-Ziv data compression algorithm.

Let $\{X_k\}_{k=-\infty}^{\infty}$ be a stationary ergodic information source with entropy H which takes values on a finite set. A typical theorem is the following. Let $l = 1, 2, \ldots$, and define the random variable $\tilde{N}_l$ as the smallest $N > 0$, such that

$$(X_0, X_1, \ldots, X_{l-1}) = (X_{-N}, X_{-N+1}, \ldots, X_{-N+l-1}).$$

Then $\frac{1}{l} \log \tilde{N}_l \to H$, in probability, as $l \to \infty$.

V.A. Zinoviev, S.N. Litsyn

Shortening of Codes

Given some binary block code $C = (n, d, N)$ with length n, minimal distance d and cardinality N, we want to construct from this code C a subcode $C_1 = (n_1, d_1, N_1)$, where $n_1 \leq n$, $d_1 \leq d$ and the cardinality N_1 is the maximal possible. One of the general constructions looks as follows. For given $C = (n, d, N)$ let character $\psi_{\underline{u}}(C)$ of C on vector $\underline{u} \in \{0,1\}^n$, $wt(\underline{u}) = h$, $\psi_{\underline{u}}(C) = \sum_{\underline{v} \in C} (-1)^{(\underline{u}, \underline{v})}$, takes his maximal value $|\psi|$. Let s, g be natural numbers such that $g \leq \min(h/2, d/2)$. Then there exists a code $C_1 = (n_1, d_1, N_1)$, $n_1 = n - h - s$, $d_1 \geq d - 2g$,

$$N_1 = \left\rfloor \frac{1}{2^{h+s}} \max_{\delta=0,1} \left\{ \sum_{i=0}^{g} \binom{h}{i} (N + (-1)^{\delta+i}\psi) \sum_{j=0}^{g-i} \binom{s}{i} \right\} \right\lfloor .$$

J. Ziv

A Bound on the Probability of an Individual Sequence Emitted by a Finite-State Source, and Applications

A lower bound on $-\log p(\underline{x})$ is derived where $\underline{x}$ is a sequence emittel by a finite-alphabet, finit-state source.

This bound is then applied to universal data compression, universal Hypothesis testing as well as to some estimation problems, yielding universal, asymptotically optimal rules for the case where the probability measures are not available.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

In all these cases the resulting asymptotically optimal rules are related to the Ziv–Lempel data compression algorithm.

Berichterstatter: K.–U. Koschnick (Bielefeld)

Gefördert durch
DFG Deutsche Forschungsgemeinschaft
©

Tagungsteilnehmer

Prof. Dr. R. Ahlswede
Fakultät für Mathematik
der Universität Bielefeld
Postfach 8640

4800 Bielefeld 1

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

Murray Hill , NJ 07974-2070
USA

Prof. Dr. S. Arimoto
Dept. of Information Physics and
Mathematical Engineering
University of Tokyo
Bunkyo-ku

Tokyo 113
JAPAN

Prof. Dr. G. Cohen
ENST
46, rue Barrault

F-75013 Paris

Prof. Dr. Th. Beth
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Haid-und-Neu-Str. 7

7500 Karlsruhe 1

Prof. Dr. M. Cohn
Dept. of Computing Science
Brandeis University

Waltham , MA 02254
USA

Prof. Dr. R. E. Blahut
IBM Corporation
Route 17C

Owego , NY 13827-1298
USA

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

H-1053 Budapest

Prof. Dr. I. Blake
Dept. of Electrical Engineering
University of Waterloo

Waterloo, Ontario N2L 3G1
CANADA

Dr. S. M. Dodunekov
Inst. of Mathematics
Bulgarian Academy of Sciences
P. O. Box 373

1090 Sofia
BULGARIA

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Prof. Dr. B. Dorsch
Signalverarbeitungsinstitut
Universität Darmstadt

6100 Darmstadt

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

S-58183 Linköping

Prof. Dr. G. Dueck
IBM Deutschland GmbH
Wissensch. Zentrum Heidelberg
Tiergartenstraße 15

6900 Heidelberg

Prof. Dr. S. I. Gelfand
Institute for Problems of Information Transmission, Academy of Sciences
ul. Ermolova 19

Moscow 101 447 GSP-4
USSR

Dr. A. Dür
Institut für Mathematik
Universität Innsbruck
Technikerstr. 25

A-6020 Innsbruck

Prof. Dr. Te Sun Han
Dept. of Information Systems
School of Business Administration
Senshu University
Higashimita 2-1-1, Tam-ku

Kawasaki-Shi, Kanagawa 214
JAPAN

Dr. I. Dumer
Institute for Problems of Information Transmission, Academy of Sciences
ul. Ermolova 19

Moscow 101 447 GSP-4
USSR

Prof. Dr. C. Heegard
School of Electrical Engineering
Phillips Hall
Cornell University

Ithaca , NY 14853
USA

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

I-10129 Torino

Dr. T. Helleseth
Institutt for Informatikk
Universitetet i Bergen
Allegaten 55

N-5007 Bergen

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

©

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

S-221 00 Lund

K. U. Koschnick
Fakultät für Mathematik
der Universität Bielefeld
Postfach 8640

4800 Bielefeld 1

Dr. H. Kleijer
Department of Mathematics
Eindhoven University
of Technology
P.O.Box 513

NL-5600 MB Eindhoven

Prof. Dr. A. V. Kuznetsov
Institute for Problems of Information Transmission, Academy of Sciences
ul. Ermolova 19

Moscow 101 447 GSP-4
USSR

Prof. Dr. T. Kløve
Institutt for Informatikk
Universitetet i Bergen
Allegaten 55

N-5007 Bergen

Prof. Dr. J. H. van Lint
Department of Mathematics
Eindhoven University
of Technology
P.O.Box 513

NL-5600 Eindhoven

Prof. Dr. K. Kobayashi
School of Electrical Engineering
Cornell University
301 Phillips Hall

Ithaca , NY 14853
USA

Prof. Dr. H. Marko
Institut für Nachrichtentechnik
Technische Hochschule München
Arcisstr. 21

8000 München 2

Dr. J. Körner
Mathematical Institute of the
Hungarian Academy of Sciences
Realtanoda u. 13 - 15
P. O. Box 127

H-1053 Budapest

Prof. Dr. J. L. Massey
Inst. f. Signal- und Informationsverarbeitung
ETH Zürich
ETH-Zentrum

CH-8092 Zürich

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

©

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

B-3030 Heverlee

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

H-1053 Budapest

Prof. Dr. P. Narayan
Electrical Engineering Department
University of Maryland

College Park , MD 20742
USA

Dr. H. Stichtenoth
FB 6 - Mathematik
Universität-GH Essen
Universitätsstr. 1-3
Postfach 103 764

4300 Essen 1

Prof. Dr. H. Noltemeier
Institut für Informatik I
Universität Würzburg
Am Hubland

8700 Würzburg

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

SF-20500 Turku

Dr. M. S. Pinsker
Institute for Problems of Information Transmission, Academy of Sciences
ul. Ermolova 19

Moscow 101 447 GSP-4
USSR

Prof. Dr. B. S. Tsybakov
Institute for Problems of Information Transmission, Academy of Sciences
ul. Ermolova 19

Moscow 101 447 GSP-4
USSR

Prof. Dr. J. P. M. Schalkwijk
Dept. of Electrical Engineering
Eindhoven University of Technology
P. O. Box 513

NL-5600 MB Eindhoven

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

NL-5600 MB Eindhoven

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

©

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

Murray Hill , NJ 07974-2070
USA

Prof. Dr. V. A. Zinoviev
Institute for Problems of Information Transmission, Academy of Sciences
ul. Ermolova 19

Moscow 101 447 GSP-4
USSR

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

Haifa 32000
ISRAEL

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

©

Gefördert durch
DFG Deutsche Forschungsgemeinschaft