MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 14/1982

Informationstheorie

5.4. bis 10.4.1982

Auf dieser Tagung, die von den Herren R. Ahlswede (Bielefeld) und J.H. van Lint (Eindhoven) geleitet wurde, standen folgende Problemkreise im Vordergrund:

- Algebraische Kodierungstheorie
- "Multi-user" Informationstheorie
- Informationstheoretische Methoden in der Statistik

Auffallend waren die erhebliche Anzahl überdurchschnittlicher Ergebnisse und der fruchtbare Gedankenaustausch zwischen Mathematikern und theoretischen Ingenieuren.

Anmerkung: Sind an den vorgestellten Ergebnissen mehrere Autoren beteiligt, so ist der Name des Vortragenden unterstrichen

Vortragsauszüge

R. AHLSWEDE, I. CSISZÁR:

Hypothesis Testing and Data Reduction

Suppose that in a testing problem for two bivariate distributions P_{XY}, Q_{XY} on finite sets the Statistician has access to the samples of one of the marginals and can be informed about those of the other one at a prescribed rate R.

Fixing the error of 1. kind e_1 at ε we consider the smallest possible error of 2. kind $e_2(n,\varepsilon,R)$ and determine its exact asymptotic growth. We also settle the composite case.

In the special case

$$H_o : Q_{XY} = P_X \times P_Y \; ; \qquad H_1 : P_{XY}$$

(Test of independence)

our result can be easily described as follows:

Theorem: For $\varepsilon \in (0,1)$

$$\lim_{n\to\infty} \frac{1}{n} \log e_2(n,\varepsilon,R_X) = - \max_{U: I(U \wedge X) \le R_X} I(U \wedge X) ,$$

where the "max" ranges over all RV's U, such that U,X,Y form a Markov-chain in this order and the range of U is bounded by $|X| + 2$. I denotes the mutual information.

The proof for this special case uses the entropy characterization technique first developed by Ahlswede/Körner in their solution of the Source Coding Problem with Side Information (IEEE 1975).

Our general results are based on the solution of an analog I-divergence characterization problem.

In the sixties Perez has introduced the notion of ε-sufficiency for the purpose of data reduction. Here for the first time asymptotically exact results for data reduction are achieved. We also think that the connection between the area of hypothesis testing and multi-user source coding should lead to a fruitful exchange of ideas and methods in Information Theory and Statistics. An important connection between Multi-user channel coding and Screening Design of Experiments can be found in the work of Maljutov and his coworkers.

M.R. BEST

Perfect Codes Hardly Exist

It is proved that all t-perfect codes over arbitrary alphabets are known, unless (possibly) $t \in \{1,2,6,8\}$. This "almost" proves the Perfect Code Theorem. The proof exploits Lloyd's Theorem, but does not refer to the sphere packing condition.

For large block lengths, it is shown that the three or four central zeros of a Kravčuk polynomial cannot be integral simultaneously. For smaller block lengths, a contradiction is derived from the system of divisibility relations

$$q^j \mid \binom{t}{j}(n-t)(n-t+1)\cdot\ldots\cdot(n-t+j-1) \quad \text{for } j \in \mathbb{N},$$

where q is the alphabet size, and n the block length.

For single and double error correcting codes, the method applied

is worthless, since the relevant Kravčuk polynomials do not have enough zeros. 6- and 8- perfect codes could be excluded using the method, although they require special treatment.

The lecture contains, of course, only outlines of the proofs.

T. BETH

Speeding up the Fast Fourier Transform by Formal Algebraic Operations

As usual Discrete Fourier Transform (DFT) of order n over a field $\mathbb{F}$ is the transformation

$$A_n : \mathbb{F}^n \to \mathbb{K}^n$$

where $\mathbb{K}$ is the splitting field of $x^n-1 \in \mathbb{F}[x]$, char $\mathbb{F} \nmid n$ and A_n is given by the matrix $A = (\alpha^{ij})_{i,j=0}^{n-1}$ for a primitive n-th root of unity.

All known Fast DFT techniques are based on decomposition properties of the group $\Gamma = \langle\alpha\rangle$ and the polynomial interpretation of the mapping.

By ADFT a method is presented, which allows a parallel implementation of the DFT-algorithm due to

- properties of the Galois group Aut ($\mathbb{K} : \mathbb{F}$),
- the choice of a suitable normal basis of $\mathbb{K} : \mathbb{F}$
- and a hardware oriented design.

ADFT computes the DFT-spectrum in O(n) steps without $\mathbb{K}$ - multiplications.

M.V. BURNASHEV

On Optimal Choice of Signals for the Channel with White Gaussian Noise

Assume that unknown parameter $\theta \in [0,1]$ and to transmit it over the channel we are able to use any signal $S_t(\theta)$, satisfying only the energy constraint

$$\int_0^T S_t^2(\theta)dt \le A \quad \text{for all } \theta \in [0,1],$$

where A is prescribed energy. On the output of the channel we observe the signal $X_t = S_t(\theta)+n_t$, $t \in [0,T]$, where n_t is the white Gaussian noise with unit density. We investigate the following function

$$e_\alpha(A) \triangleq \inf_{S,\hat{\theta}} \sup_{\theta \in [0,1]} E_\theta |\hat{\theta}-\theta|^\alpha,$$

where inf is taken over all possible signals S_t and estimators $\hat{\theta} = \hat{\theta}(X_0^T)$. It's easy to see that $e_\alpha(A) \sim \exp\{-\gamma(\alpha)A\}$, when $A \to \infty$, and therefore we are interested in the function $\gamma(\alpha)$.

Theorem: a) $\gamma(\alpha) = \frac{\alpha}{4(\alpha+1)}$ for $\alpha > 2{,}17$;

b) $\frac{1}{6} \le \gamma(2) \le \frac{1}{5{,}996}$.

P. CAMION

Constructing Primitive Idempotents and Factorizing Polynomials over Finite Fields

Let A be a semi-simple commutative algebra of finite dimension over a finite field. A probabilistic algorithm for decomposing an idempotent u of A into a sum of primitive idempotents is first introduced.

Then some properties of finite fields are pointed out which lead to improve the considered algorithm and ensure that it will then end within a number of steps which is small compared to the size q of the field.

An application to factorizing polynomials over a finite field is considered and more particularly to finding the roots of such polynomials in view of decoding B.C.H. codes. The complexity of the algorithm is finally discussed.

References

P. Camion: "Un algorithme de construction des idempotents primitifs d'idéaux d'algèbres sur $\mathbb{F}_q$" C.R. Acad. Sc. Paris t. 291(20 octobre 1980)
Under the same title, a larger paper submitted july 1980 is to appear in Theory and Practice of Combinatorics, Annals of Discrete Mathematics, 1982.

P. Camion: "A Deterministic Algorithm for Factorizing Polynomials of $\mathbb{F}_q[x]$". To appear in the proceedings of the "Colloque Combinatoire 81.", Marseille Luminy. Annals of Discrete Mathematics

P. Camion: "Factorisation des polynômes de $\mathbb{F}_q[x]$" Revue du CETHEDEC, N.S. 812, 4ème, trimestre 1981.

N. COT

Codes, Results and Conjectures Associated with Some Weighted Trees

We start with Shannon's well-known general problem concerning the discrete noiseless memoryless channel.

Given

- a t-ary alphabet $A = \{ a_1, a_2, \ldots, a_t \}$
- a set of positive costs $B = \{ b_1, b_2, \ldots, b_t \}$
- a set of probabilities $P = \{ p_1, p_2, \ldots, p_n \}$,

(i) characterize optimal Uniquely Decipherable (U.D.) codes,

(ii) design efficiently optimal UD codes.

In this talk, we make a survey of various results we have obtained concerning this problem. In particular, in the case where probabilities are all equal, we showed in 1974 that optimal prefix codes can be nicely represented by subsets of Pascal's triangle. We indicate various applications of optimal prefix codes in computer science (AVL trees, polyphase merging, etc. ...). Also, studying the properties of the corresponding weighted trees, we achieve various results concerning binomial coefficients lying on the diagonals of Pascal's triangle.

Most references to these results can be found in the thèse d'état "Combinatoire des arbres t-aires dont les branches ont des coûts positifs quelconques", Norbert Cot, Université Pierre et Marie Curie (Paris, France).

B. DORSCH

The Problem of Attaining Channel Capacity by Algebraic Coding/Decoding

After asymptotically good long algebraic codes are known (e.g. Goppa-codes or some generalizations of BCH-codes) the problem is mainly that of decoding. Three decoding principles will be compared: 1) Max. Lik. Dec. (MLD) with almost no hope for realization (complexity ~ exp (N)), 2) Practical algebraic decoding (with complexity ~ NlogN) using Bounded Minimum Distance Decod. (BMD), which can not attain capacity. But there is some hope to extend BMD-procedures beyond half minimum distance. The decoding principle of this type 3) is compared to MLD and BMD. By deriving error exponents numerical results are given for the Binary Symmetric Channel (BSC) and Additive White Gaussian Noise (AWGN), showing that

- for $N \to \infty$, $P_e \to 0$ the code rate R of 3) does not only approach capacity, but P_e converges as fast to zero as with MLD for rates R close to capacity.
- for finite N, P_e type 3) decoding is much better that BMD and almost as good as MLD.

Some detailed algebraic problems involved in finding decoding procedures of type 3) for asymptotically good generalizations of BCH-codes are discussed.

T. ERICSON

The Non-Cooperative Binary Adder Channel

The binary adder channel is a multiple access channel with two binary inputs, X and S say, and a ternary output $Y = X + S$. We are interested in the non-cooperative untilization of this channel, where X denotes a legal user, the aim of which is to minimize his word error probability, while S represents an illegal jammer, whose aim is the opposite. For this situation we formulate a two persons zero sum game, which can be solved in certain cases. Our approach is based on algebraic coding.

L. GYÖRFI, I. KEREKES

Analysis of a Multiple Access Channel Using Multiple Frequency Bands

For a multiple frequency communication scheme an information theoretic model and its analysis are given.
The corresponding multiple access channel consists of several independent, parallel, noisy OR channels. A block code and a majority type decoding rule is constructed, and the probability of error is evaluated.

Y. HORIBE

On Fibonacci Trees and Their Optimality

Based on some results in a previous paper "An entropy view of Fibonacci trees", Fibonacci Quarterly, May 1982, we classify

the terminal nodes of Fibonacci trees (F-trees for short) into two types. Branching all nodes of the first type grows the F-tree of order k into the one of order $k + 1$ ("Fibonacci growth"). The numbers of nodes of each type at each level of F-trees are shown to be diagonally arranged in the Pascal triangle. Let cost 1 be assigned to every left branch and cost c to every right, and define total cost of a binary tree to be the sum of costs of all terminal nodes, here the cost of a node being the sum of costs of branches forming the path from the root to this node. Necessary and sufficient condition on k,c is then given, together with its entropic interpretation, for the F-tree of order k to be optimal (i.e., to have the minimum total cost) of all binary trees having the same number of nodes. The total cost of the F-tree of order k under the above cost assignment is obtained exactly. These with previous ones might give hints also to a "morphological" study of some other types of binary trees.

J. KÖRNER, J. K. WOLF, A. WYNER, J. ZIV

On the Capacity of a Reusable Nonerasable Memory

A memory consisting of N binary storage elements is to be utilized to store K binary messages. The memory is characterized by the fact that a "one" stored in a storage element is non-erasable- that is, cannot be changed to a "zero". The memory is initially in the all zero state and the messages are stored sequentially in time. After the i th message is stored

in memory, it is assumed that this i th message can be read from memory with arbitrarily small probability of error but that the $(i-1)$ previous messages are no longer readable at arbitrary small error rates.

The capacity of the memory is defined as the maximum sum of the rates for the K messages. The capacity of the system is found for several different sets of assumptions regarding the devices that write in and read from the memory.

R. D. BAKER, J. H. VAN LINT, R. M. WILSON

Preparata and Goethals Codes

Let m be odd, $n = 2^m-1$, $\mathbb{F} := GF(2^m)$, $x \to x^\sigma$ an automorphism of $\mathbb{F}$ such that $x \to x^{\sigma+1}$ and $x \to x^{\sigma-1}$ are one-to-one. Codewords of the code $\overline{P}(\sigma)$ are described by pairs $(X,Y) \in \mathbb{F} \times \mathbb{F}$ to be interpreted as the corresponding characteristic functions. The code $\overline{P}(\sigma)$ is defined by the requirements

(i) $|X|$ and $|Y|$ are even

(ii) $\Sigma x = \Sigma y$

(iii) $\Sigma x^{\sigma+1} + (\Sigma x)^{\sigma+1} = \Sigma y^{\sigma+1}$.

(N. B. It is easy to check that the usual definition of the Preparata codes amounts to the same, with $\sigma = 2$).

It is now completely elementary to prove:

$\overline{P}(\sigma)$ is translation invariant;

Aut $\overline{P}(\sigma)$ contains the mappings from (X,Y) to resp. $(X+c,Y+c)$, (Y,X), $(\alpha X,\alpha Y)$, $(X^{\varphi},Y^{\varphi})$, $(\varphi \in \text{Aut } \mathbb{F})$;

$\overline{P}(\sigma)$ has distance 6 ;

$|\overline{P}(\sigma)| = 2n - 2m$.

We also show in an elementary way that the ext. Hamming code is a disjoint union of translates of $\overline{P}(\sigma)$ (first proved by Zaitsev, Zinoviev, Semakov). If $m = 2t+1$, $\sigma = 2^t$, $\rho = 2^{t-1}$ then the Goethals code $\overline{G}(m)$ is $\overline{P}(\sigma) \cap \overline{P}(\rho)$. It is again easy to show (using the Roos-bound) that $\overline{G}(m)$ has distance 8 .

K. MARTON

The Problem of Isomorphy of Correlated Sources

A discrete memoryless stationary correlated (DMSC) source (X,Z) is an i.i.d. sequence of random pairs $\{(X_i,Z_i)\}_{i=-\infty}^{\infty}$ with values in $X_0 \times Z_0$, where X_0 and Z_0 are finite sets. Two DMSC sources (X,Z) and (X',Z') are isomorphic if there exists an ergodic theoretic isomorphism between the Bernoulli processes (X,Z) and (X',Z') , the restrictions of which are isomorphisms between X and X' , resp. Z and Z' . It is well known that two "single" discrete memoryless stationary sources are isomorphic iff their Shannon entropies are equal.

We prove, however, that under quite general conditions, the DMSC sources (X,Z) and (X',Z') are isomorphic only if (X_0,Z_0) and (X_0',Z_0') are, i.e. if $\text{dist}(X_0,Z_0) = \text{dist}(X_0',Z_0')$. (The general case can be reduced to this result.) From the point of view of generalizations, it would be desirable to find "entropy type" invariants for the isomorphy of (X_0,Z_0) and (X_0',Z_0'), and we present some partial results in this direction.

J. L. MASSEY

Capacity and Coding for the Collision Channel without Feedback

The channel considered is the M-user time-slotted collision-channel without feedback and without synchronization. Each of the M users can be idle or can transmit a "packet" of data. If two or more users send packets that overlap, these "colliding" packets completely destroy one another. Otherwise, packets are correctly received. The lack of synchronization means that no user knows the "time origins" chosen by the other users.

The "symmetric capacity" (i.e., the maximum total rate at which the users can send information reliably when each sends at the same rate) is shown to be

$$C = \left(1 - \frac{1}{M}\right)^{M-1} \quad \text{packets/slot}$$

which rapidly approaches e^{-1} as M increases. Specific trans-

mission schemes or "protocols" that achieve capacity are introduced and a decoding technique, called "decimation decoding" is developed for identifying the origin of those packets that are correctly received.

J. L. MASSEY

On the Possibility of Full Cooperation with Inclomplete Information

Consider the M-user adder channel with feedback. The channel output Y is the real sum $X_1 + X_2 + \ldots + X_M$ of the $\{0,1\}$-valued input digits. Suppose the M users all send independent uncoded information bits. If $Y = 0$ or $Y = M$, then the receiver can determine all M transmitted bits; otherwise, there is ambiguity. Consider only coding schemes of the type where, after A such ambiguous receptions have occurred, the senders use the feedback information to cooperate in transmitting the missing information to the receiver. The question is whether the M users can cooperate fully in the sense that their further transmissions cause the resulting received sequences to form an $(M + 1)$-ary Huffman code for the missing information -- as they could do if each sender knew what the other $M - 1$ senders had sent on each ambiguous reception. This complete information is available when and only when $M = 2$ -- this is the basis of the Gaarder-Wolf coding scheme. When $M \geq 4$, it is shown that full cooperation is impossible; $A = 1$ provides the necessary counterexample. It is shown that, for $M = 3$, full

cooperation is possible when A is 1, 2 or 3; the schemes for $A = 2$ and $A = 3$ are due to T. Paul. It is conjectured that, for $M = 3$, full cooperation is possible for all A.

E.C. VAN DER MEULEN

Some Results in Entropy-Based Statistical Inference

Within Information theory the problem of estimating the entropy of a distribution is well-known. In the discrete case Shannon (1951) found bounds on the entropy of printed English which he considered as a finite alphabet ergodic process. For i.i.d. observations from a discrete distribution entropy estimates were considered and investigated by Miller and Madow (1954), Basarin (1959), Zubkov(1973) and Harris (1977). In 1976 O. Vasicek proposed an estimate of the entropy of a continuous distribution based on the spacings of the observations. Vasicek developed a test for composited normality and proved consistency for this estimator. Dudewicz and van der Meulen (1981) investigated the use of the Vasicek test statistic for testing the hypothesis of uniformity on (0,1). They introduced a test (the entropy-based test) for unformity which rejects when the test statistic $H(m,n)$ is small (i.e. large negative). The percentiles of the null distribution are obtained through extensive Monte Carlo simulation. The power of the teststatistic is studied, also through Monte Carlo, against three types of alternatives. It turns out that among all well-known tests (Kolmogorov-Smirnov, etc.,) the entropy-based test has highest power when

the density is peaked up in the middle of the (0,1)-interval. The asymptotic distribution of the teststatistic is found to be normal, under the hypothesis of uniformity, and also under the alternative that the density is a bounded positive step-function on (0,1). Applications are given towards the problem of evaluating random number generators.

A. PEREZ

A General Information Theory Method Covering Coding Rate Versus Ambiguity as Well as Statistical Hypotheses Discrimination Rate Problems for Unfitted Decision Procedures

Restricting us for the sake of simplicity to the i.i.d. case the Fundamental Lemma is:

Let $P \ll Q$ on $(X,\mathcal{X})$ and let, for a real γ, $Q_\gamma := Qe^\gamma$, where P and Q $(P \neq Q)$ are probability measures with Radon-Nikodym densities p and q with respect to a dominating measure μ. Let

(1) $H_\alpha(P,Q_\gamma) := \int p^\alpha(x) q_\gamma^{1-\alpha}(x) d\mu = \int p^\alpha(x) q^{1-\alpha}(x) e^{\gamma(1-\alpha)} d\mu = H_\alpha(P,Q) e^{\gamma(1-\alpha)}$,

and let $\alpha(P,Q_\gamma)$ be the α minimizing $H_\alpha(P,Q_\gamma)$. It holds:

(2) $\alpha(P,Q_\gamma) \lesseqgtr 1$ iff $\gamma \lesseqgtr H(P,Q) := \int \log \frac{dP}{dQ}\, dP > 0$

(3) $\alpha(P,Q_\gamma) \lesseqgtr 0$ iff $\gamma \lesseqgtr -H(Q,P) < 0$

(4) $\Delta(P,Q_\gamma) := \log H_{\alpha(P,Q_\gamma)}(P,Q_\gamma) = \log H_{\alpha(P,Q_\gamma)}(P,Q) + (1-\alpha)\gamma \leq 0$

with $\Delta(P,Q_\gamma) = 0$ iff $\gamma = H(P,Q)$.

If $-H(Q,P) \leq \gamma \leq H(P,Q)$ (i.e. $0 \leq \alpha(P,Q_\gamma) \leq 1$) then

$$(5)\quad \lim_{n\to\infty} \frac{1}{n} \log P^n\left(\frac{1}{n} \sum_{i=1}^{n} \log \frac{dP}{dQ}(x_i) \leq \gamma\right) =$$

$$= \lim_{n\to\infty} \frac{1}{n} \log Q_\gamma^n\left(\frac{1}{n} \sum_{i=1}^{n} \log \frac{dP}{dQ}(x_i) > \gamma\right) = \Delta(P,Q_\gamma)$$

If only $\gamma \leq H(P,Q)$ (i.e. $\alpha(P,Q_\gamma) \leq 1$) then

$$(6)\quad \limsup_{n\to\infty} \frac{1}{n} \log P^n\left(\frac{1}{n} \sum_{i=1}^{n} \log \frac{dP}{dQ}(x_i) \leq \gamma\right) \leq \Delta(P,Q_\gamma)$$

J. POKORNY, H.-M. WALLMEIER

Permutationcodes Achieve the Capacity Regions for the MAC and DBC

For a discrete memoryless channel Ahlswede/Dueck have shown that any rate below capacity can be achieved by permutation -codes. Codewords are constructed by applying (or not applying) a (randomly chosen) set of permutations $\{\pi_1,\ldots,\pi_m\}$ to an arbitrary given sequence x^n of type P, thus producing new sequences

$$\pi_m^{s_m} \circ \ldots \circ \pi_1^{s_1}(x^n) \quad , \quad s = (s_1,\ldots,s_m) \in \{0,1\}^m.$$

We show, that the capacity regions for the multiple-access-channel and the degraded broadcast-channel are achievable by constructing codewords via permutations.

K. POST

Coding Strategies for the Binary Multiplying Channel in the Discrete Case

A first approach is given to minimize the average number of transmissions needed on the BMC with feedback to transmit every message pair

$(\theta_A,\theta_B) \in \{1,2,\ldots,M\} \times \{1,2,\ldots,N\}$. For $M = 1,2,3$ and arbitrary N this minimum is found by Hollmann and Post. In particular for M=3 Hollmann found better strategies than those obtained by using Schalkwijk's method. As an application the case M=N=11 admits better non-Schalkwijk strategies than Schalkwijk-strategies.

V. V. PRELOV

The Zero-Error Capacity of Certain Channels

In this report we consider a multiple-access communication system with the correlated sources, which were first studied by Slepian and Wolf in 1973.
Denote by R the capacity region of this multiple access channel and denote by R_0 the zero-error capacity region of this channel. Let $R^{(i)}$ ($R_0^{(i)}$) be the intersection of the region R (R_0) with the plane $R_i = 0$, $i = 0,1,2$. The simple characterization of the capacity region R is given by Slepian and Wolf. The simple characterization of the zero-error regions

R_0 and $R_0^{(o)}$ remains the open problem. The following theorem is a main result.

Theorem: For the arbitrary deterministic multiple access channel the following equality $R^{(i)} = R_0^{(i)}$, $i = 1,2$, is valid. (A multiple access channel is the deterministic channel if its transition probabilities are equal to zero or one.)

C. ROOS

A Generalization of the BCH Bound for the Minimum Distance of a Cyclic Code, Also Improving the Hartmann-Tzeng Bound

Let K be any finite field. For any matrix $A = [\underline{a}_1,\ldots\underline{a}_n]$ over K, the code over K having A as a parity check matrix is called C_A, its min. dist. is d_A. If $X = [\underline{x}_1,\ldots,\underline{x}_n]$ is another matrix over K, with size $m \times n$, then the matrix $A(X)$ is defined as $A(X) := [\underline{x}_1 \otimes \underline{a}_1,\ldots,\underline{x}_n \otimes \underline{a}_n]$. All columns in A and X are nonzero.

Theorem 1: If every $m \times (d_A + m - 2)$ submatrix of X has full rank, then $d_{A(X)} \geq d_A + m - 1$.

Now let M and N be nonempty sets of n-th roots of unity in the field K. Let H_N be a matrix whose rows are $(\alpha,\alpha^2,\ldots,\alpha^n = 1)$, $\alpha \in N$. Further, let $C_N := C_{H_N}$ and $d_N := d_{H_N}$. Call the set M consecutive if its elements are consecutive powers of some primitive n-th root of unity.

Theorem 2: If there exists a consecutive set $\overline{M}$ such that $M \subset \overline{M}$ and $|\overline{M}| \leq |M| + d_N - 2$, then $d_{MN} \geq |M| + d_N - 1$.

Corollary: If N is consecutive and $|\overline{M}| < |M| + |N|$, then

$$d_{MN} \geq |M| + |N| .$$

Taking $M = \{1\}$ in the corollary yields the BCH bound. Similarly, the Hartmann-Tzeng bound follows by taking for M a consecutive set.

J. P. M. SCHALKWIJK

Coding Strategies for Deterministic Multi-User Channels

We consider coding strategies for deterministic multi-user channels, i.e. for a memory with known defects, for a multiple-access channel (MAC), for a broadcast channel (BC), and for a two-way channel (TWC).
For the TWC we use a coding technique that we called coding on the unit square.

A. SGARRO

Error Probabilities for Simple Substitution Ciphers

Usually the performance of simple substitution ciphers is evaluated by considering equivocations (conditional entropies given the cryptogram). Instead we consider the probability that the enemy makes an error when he tries to decipher the cryptogram or to identify the key by means of optimal identification procedures. This approach is in line with the usual approach to coding problems taken in Shannon theory, where one evaluates error probabilities with respect to "good" encoding-decoding procedures. The results are asymptotic; the same relevant parameters are obtained as with the equivocation approach.

H. VAN TILBORG

Upperbounds and a Construction for the 2-Access Binary Adder Channel

Let (C_1,C_2) be a uniquely decodable code for the two-access binary adder channel.

For a given C_1 an algebraic and a combinatorial upperbound is derived on $|C_2|$. For many classes of codes the algebraic upperbound can easily be computed. For a specific code C_1 one can often use the combinatorial upperbound to get better estimates.

For a specific code C_1 of size 6 and length 5 this combinatorial upper bounding technique gives additional information on C_2. We construct in this way a uniquely decodable pair (C_1,C_2) with a rate pair above the nonconstructive lower bound found by Wei, Kasami, Lin and Yamamura. The size of this code C_2 is 15.

D. TOWSLEY, J. K. WOLF

Group Testing and Multi-Access Communications

The work of Dorfman, Sterrett, and Sobel and Groll were reviewed with respect to traditional group testing. A finite number of items with a binomial distribution for defects was assumed. A new model was described whereby the result of each test indicated one of three outcomes: no defects, one defect

(which is identified) and more than one defect. A nested testing procedure for this model and a method for finding the optimum parameters for this procedure was described. This method yields the average number of tests for this procedure in terms of the number of items N and the parameter p of the binomial distribution.

F. M. J. WILLEMS

Backward Decoding for the Discrete Memoryless Multiple Access Channel with Generalized Feedback

We introduce backward decoding as a method to obtain a simultaneous form of decoding if block Markov superposition encoding is used. Applying these techniques we prove that for the d.m. MAC $(X_1 \times X_2, P^*(y,y_1,y_2|x_1,x_2), Y \times Y_1 \times Y_2)$ in the generalized feedback situation the region R_{gf} is achievable where

$$R_{gf} \triangleq \{(R_1,R_2) : R_1 = R_{12} + R_{11},\ R_2 = R_{21} + R_{22},$$
$$0 \le R_{12} \le I(V_1;Y_2|X_2,U),\ 0 \le R_{21} \le I(V_2;Y_1|X_1,U),$$
$$0 \le R_{11} \le I(X_1;Y|X_2,V_1,U),$$
$$0 \le R_{22} \le I(X_2;Y|X_1,V_2,U),$$
$$R_{11} + R_{22} \le I(X_1,X_2;Y|V_1,V_2,U),$$
$$R_{12} + R_{21} + R_{11} + R_{22} \le I(X_1,X_2;Y) \quad \text{for some}$$
$$P(u)P(v_1|u)P(v_2|u)P(x_1|v_1,u)P(x_2|v_2,u)P^*(y,y_1,y_2|x_1,x_2)\}.$$

Finally by making substitutions in R_{gf} we demonstrate how various achievablility proofs for the MAC and relay channel follow from the above result.

V.A. ZINOVIEV

Equal-Weight Codes and Maximal Packings

Let $A(n,2\delta,w)$ denote the maximal possible power of the binary equal-weight code of length n, distance 2δ and weight of codewords w. It is known (Johnson upper bound):

$$A(n,2\delta,w) \leq \binom{n}{w-\delta+1} / \binom{w}{\delta - 1}.$$

One of the results is the following theorem.

Let q be a prime power such that $q + 1 \geq w$. Then for any δ, $1 \leq \delta \leq w$, and $n = q \cdot w$

$$A(n,2\delta,w) \geq \left(\frac{n}{w}\right)^{w - \delta + 1}.$$

This bound differs from the upper bound only by the multiplier $\frac{w-1}{w} \cdot \frac{w-2}{w} \cdots \frac{\delta}{w}$.

Let $w \to \infty$ and $n_w = q_w \cdot w$, where q_w is the smallest prime power such that $q + 1 \geq w$. Then, if $w - \delta + 1 = o(w^{1/2})$

$$\lim_{w\to\infty} A(n_w,2\delta,w) \binom{w}{\delta-1} / \binom{n}{w-\delta+1} = 1.$$

Berichterstatter: Jutta Pokorny

Liste der Tagungsteilnehmer

R. Ahlswede
Department of Mathematics
University of Bielefeld
D-4800 Bielefeld 1
West Germany

M.R. Best
National Aerospace Laboratory NLR
P.O. Box 153
NL-8300 AD Emmeloord
The Netherlands

T. Beth
Informatik I, Universität Erlangen
Martensstr. 3
D-8520 Erlangen
West Germany

K. De Bruyn
K.U. Leuven-Kandidatuurcentrum
Celestijnenlaan 200A
B-3030 Heverlee
Belgium

M. Burnašev
Inst. for Probl. of Inf. Transmission
USSR Academy of Sciences
19 Ermolovoy str.
101447 Moscow
USSR

P. Camion
Centre National de la Recherche
Scientifique, Paris, Inst. National
de Recherche en Inf. et Automatique
INRIA, Le Chesnay
F-78 Rocquencourt, France

N. Cot
Institut de Programmation
Université de Paris VI
4, Place Jussieu
F-75230 Paris - 5
France

B. Dorsch
Deutsche Forschungs-und Versuchsanstalt
für Luft- und Raumfahrt (DFVLR)
D-8031 Weßling
West Germany

G. Dueck
Department of Mathematics
University of Bielefeld
D-4800 Bielefeld 1
West Germany

T. Ericson
Dep. Electrical Engineering
University of Linköping
S-58183 Linköping
Sweden

L. Györfi
Technical University of Budapest
Stoczek u. 2
H-1111 Budapest
Hungary

Y. Horibe
Department of Information Sciences
Faculty of Engineering
Shizuoka University
Hamamatsu, 432
Japan

I. Ingemarsson
Department of Electrical Engineering
University of Linköping
S-58183 Linköping
Sweden

E.C. van der Meulen
Department of Mathematics
K.U. Leuven, Celestijnenlaan 200B
B-3030 Heverlee
Belgium

I. Kerekes
Technical University
Stoczek 2
H-1111 Budapest
Hungary

T. Nemetz
Mathematical Institute of the Hungarian
Academy of Sciences
Reáltanoda u. 13-15
H-1053 Budapest
Hungary

J. van Lint
Dep. of Mathematics and Computing Science
Eindhoven University of Technology
P.O. Box 513
Eindhoven, Netherlands

A. Perez
Czechoslovak Academy of Sciences
Institute of Inf. Theory and Automation
Pod vodarenskou věži 4
182 08 Prague 8
Czechoslovakia

G. Longo
Istituto di Elettronica
Universitá di Trieste
I - 34100 Trieste
Italy

J. Pokorny
USP Mathematisierung
University of Bielefeld
D-4800 Bielefeld 1
West Germany

K. Marton
Mathematical Institute of the Hungarian
Academy of Sciences,
Reáltanoda u. 13-15
H-1053 Budapest
Hungary

K. Post
Department of Mathematics and
Computing Science
Eindhoven University of Technology,
Eindhoven, Netherlands

J.L. Massey
Institut für Fernmeldetechnik
ETH-Zentrum
CH-8092 Zürich
Switzerland

V.V. Prelov
Institute for Probl. of Inf. Transmission
USSR Academy of Sciences
19 Ermolovoy str.
101447 Moscow
USSR

C. Roos
Department of Mathematics
Delft University of Technology
Delft, Netherlands

H.-M. Wallmeier
Institute of Mathematical Economics(IMW)
University of Bielefeld
D-4800 Bielefeld 1
West Germany

J.P.M. Schalkwijk
Department of Electrical Engineering
Eindhoven University
P.O. Box 513
5600 MB Eindhoven
Netherlands

F. Willems
K.U. Leuven, Dept. Wiskunde
Celestijnenlaan 200 B
B-3030 Heverlee
Belgium

A. Sgarro
Istituto di Matematica and Istituto
di Elettrotecnica e di Elettronica
Università degli Studi di Trieste
I-34 100 Trieste
Italy

J. Wolf
Dept. of Electrical and Computer
Engineering
University of Massachusetts
Amherst, Massachusetts 01003
USA

H. van Tilborg
Dept. of Math. and Comp. Science
Eindhoven University of Technology
Eindhoven
Netherlands

L. Wolters
Department of Mathematics
University of Bielefeld
D-4800 Bielefeld 1
West Germany

H. Vinck
Department of Electrical Engineering
Eindhoven University of Technology
Eindhoven
Netherlands

V.A. Zinoviev
Inst. for Probl. of Inf. Transmission
USSR Academy of Sciences
19 Ermolovoy str.
101447 Moscow
USSR