MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 20/1986

Information Theory

11.5. bis 17.5.1986

The conference was organized by R. Ahlswede (Bielefeld), J.H. van Lint (Eindhoven), and J. Massey (Zürich).

The main subjects were algebraic coding, cryptography, and multi-user information theory. The program included 38 lectures and a discussion about open problems and recent developments.

Abstracts

T. Klöve

Some convolutional self-ortogonal codes

An (I,J) difference triangle set (DTS) is a set

$$\Delta = \{\Delta_1, \Delta_2, \ldots, \Delta_I\}$$

where

$$\Delta_i = \{a_{ij} \mid 0 \le j \le J\} \quad \text{for} \quad 1 \le i \le I$$

are sets such that all the numbers $a_{ij} - a_{ij'}$, with $1 \le i \le I$ and $0 \le j' < j \le J$ are distinct. Let

$$m(\Delta) = \max\{a_{ij}\}.$$

$$M(I,J) = \min\{m(\Delta) \mid \Delta \text{ is an } (I,J) \text{ DTS}\}.$$

We show that

$$3I \le M(I,2) \le 3I + 1 \quad \text{for all} \quad I,$$

$$M(I,2) = 3I + 1 \quad \text{for} \quad I \equiv 2 \text{ or } 3 \pmod 4.$$

$78s + 6k \le M(13s+k,3) \le 86s + c_k$ where c_k is given by the following table:

k	1	2	3	4	5	6	7	8	9	10	11	12	13
c_k	13	23	27	32	40	46	54	58	68	72	73	90	91

R. Calderbank

Applications of coding theory to designs

Theorems of Gleason and of Mallows and Sloane characterize the weight enumerator of maximal self-orthogonal codes with all weights divisible by 4. We apply these results to give a new necessary condition for the existence of quasi-symmetric $2\text{-}(v,k,\lambda)$ designs where the intersection numbers s,t satisfy $s \equiv t \pmod 2$ (the assumption that there are 2 intersection numbers can be weakened to intersection numbers $s_1, \ldots, s_n$ satisfying $s_1 \equiv \ldots \equiv s_n \pmod 2$).

We also apply duality in the Johnson scheme $J(v,k)$ to give a very short proof of a theorem of Frankl and Füredi. We consider a family $\mathcal{F}$ of k-subsets of a v-set such that $\mathcal{F}$ is a 1-design and $|x \cap y| \ge \lambda > 0$ for all $x,y \in \mathcal{F}$. We prove that $v \le (k^2-k+\lambda)/\lambda$ and that $v = (k^2-k+\lambda)/\lambda$ if and only if $\mathcal{F}$ is a symmetric $2\text{-}(v,k,\lambda)$ design.

E.F. Assmus, jr.

Self-dual binary codes and desarguesian planes of even order

Consider the code generated by the Desarguesian projective plane of order 2^e extended by an overall parity check, C say. C is self-orthogonal and we ask whether or not there is a self-dual code $S \supseteq C$ with a generator matrix of the form $(I_k|M)$ where I_k is the identity matrix and M is a $k \times k$ matrix that is the incidence matrix of a biplane. Here $k = \frac{1}{2}(2^{2e}+2^e+2)$. The answer for $e = 1,2$, and 3 is yes and there is a general group theoretic construction that yields M in these cases. This same construction yields matrices M for $e > 3$ that have the property that every row has $2^e + 1$ ones and every two rows have 0,2, or 4 ones in common, but for no $e > 3$ is M the incidence matrix of a biplane.

J.P.M. Schalkwijk

Two-way channels

Shannon's (1961) model of a two-way communication channel is discussed, in particular the inner and outer bounds to the capacity region. As an example of a nontrivial dialogue we then consider Blackwell's binary multiplying channel (BMC), as does Shannon in his own two-way channel paper refered to above. We describe Schalkwijk's (1983) coding strategy for the BMC, which we subsequently show to be optimum for both fixed length strategies with vanishing probability of error, and also for variable length strategies with zero probability of error. Thus we establish for the first time the capacity region of a nontrivial (i.e. inner $\neq$ outer bound) two-way channel. For symmetric $R_1 = R_2$ operation the optimum rate is $R_1 = R_2 = .63056$ bit per transmission. The essential step in the converse considers the uncertainty reduction for resolutions on the initial threshold pair of the (θ_1,θ_2)-search on the unit square.

A.M. Odlyzko

Balancing sets of vectors

This lecture was based on joint work with E. Bergmann, D. Coppersmith, and P. Shor. Given a positive integer n, what is the minimal value of k such that there exist k vectors $\underline{v}_1,\ldots,\underline{v}_k$ of length n with entries ± 1 such that for any vector $\underline{w}$ of length n with entries ± 1, there is at least one i, $1 \le i \le k$, with $\underline{v}_i \cdot \underline{w} = 0$?

A very simple construction due to Knuth shows that $k \le n$ is possible, and a proof using commutative algebra is given that $k = n$ is best possible. This construction and its extensions have many applications to communication theory.

Z-x. Wan

On the relationship between Berlekamp-Massey and Euclidean algorithms for synthesizing binary sequences

Let $\underline{a} = (a_0,a_1,\ldots,a_{N-1})$ be a binary sequence with $a_0 = a_1 = \ldots = a_{n_0-1} = 0$, $a_{n_0} = 1$. Put $r_0(x) = \sum_{i=0}^{N-1} a_{N-1-i}x^i$, $r_{-1}(x) = x^N + r_0(x)\varepsilon(x)$, where $\varepsilon(x)$ is an arbitrary polynomial of degree $\le n_0$, and also put $W_0(x) = 1$, $W_{-1}(x) = \varepsilon(x)$. Define $r_k(x)$ and $W_k(x)$ $(k=1,2,\ldots)$ inductively as follows: $r_k(x) = p_k(x)r_{k-1}(x) + r_{k-2}(x)$, where $\deg r_k(x) < \deg r_{k-1}(x)$ and $W_k(x) = p_k(x)W_{k-1}(x) + W_{k-2}(x)$. Suppose k is the smallest positive integer such that $\deg r_k(x) + \deg r_{k-1}(x) < N$, then $W_k(x)$ is a shortest LFSR which generates $\underline{a}$. This is the so-called Euclidian algorithm for synthesizing binary sequences.

For $k = 1,2,\ldots,$ write $p_k(x) = \sum_{i=1}^{w_k} x^{\lambda_{ki}}$ where $\lambda_{ki} > \lambda_{ki+1}$, $i = 1,2,\ldots,w_{k-1}$. Then put $p_{k\tau}(x) = \sum_{i=1}^{\tau} x^{\lambda_{ki}}$, $W_{k\tau}(x) = p_{k\tau}(x)\,W_{k-1}(x) + W_{k-2}(x)$. Order the set $\{(k,\tau)\mid 1\le k\le n,\ 1\le\tau\le w_k\}$ lexicographically: $(k,\tau) < (k',\tau')$ iff $k < k'$ or $k = k'$, $\tau < \tau'$. Then we have the sequence of polynomials

$$W_{11}, W_{12}, \ldots, W_{1w_1} (=W_1), W_{21}, W_{22}, \ldots, W_{2w_2} (=W_2), \ldots, W_{k1}, W_{k2}, \ldots, W_{kw_k} (=W_k), \ldots .$$

It is proved that by adding n_0 1's in front of W_{11} and repeating each $W_{k\tau}$ a certain number of times, we obtain the sequence of polynomials obtained by the Berlekamp-Massey algorithm.

Ingemar Ingemarsson

Further results on unknown functions

An invertible function $y = f(x)$, where x and y are integers in the range $[1,n]$, is chosen from a set F of M functions. An outside observer knows F but not the actual choice $f(x)$. He is however able to make a limited number, say i, of observations (x,y) satisfying the unknown function. He concludes that the function is in a subset of F. If there are equally many functions in this subset attaining each possible value y for any argument x the observer is said to have maximal uncertainty at level $i + 1$. The highest level with maximal uncertainty is called the security level k of F. The largest security level, k, satisfies $M = \frac{n!}{(n-k!)}$. Functions with maximal security level are closely related to Reed-Solomon-codes.

If the functions in F are chosen randomly the security level is far from maximal.
The cascading of two unknown functions, i.e. $f[f(x)]$ is discussed.

I. Csiszár and P. Narayan

Arbitrarily varying channels with jamming constraints

Given an AVC with jamming constraint $\sum_{i=1}^{n} \rho(s_i) \leq \alpha n$, let C_r and C_a denote the average error capacity for random and non-random block codes, respectively. While a single-letter formula for C_r is available, now the "elimination technique" does not work, by which Ahlswede proved in the unconstrained case that $C_a = C_r$ unless $c_a = 0$. Here we determine C_a for deterministic channels with binary input and jammer alphabets; it turns out that $0 < C_a < C_r$ may also obtain. If $Y = X + S \bmod 2$ then $C_a = C_r = 1-h(\alpha)$; the problem of maximum error capacity for this

case is identical with the basic open problem about error-correcting codes. The case $Y = X \cdot S$ represents a model for memories with defects of unknown locations. A partial result is obtained for Gaussian AVC's, namely that $C_a = C_r$ for a certain range of the parameters; it remains unknown whether this always holds when $C_a \neq 0$.

F.M.J. Willems

A new universal data compression method

A new universal data compression algorithm is described. This algorithm encodes L source symbols at a time. The code alphabet is binary. For the class of binary stationary sources, the expected number of code symbols per source symbol is shown to be not more than $(H(U_0,U_1,\ldots,U_{L-1}) + \lceil \log(L+1) \rceil)/L$. In the analysis of our algorithm a result on repetition times turns out to be crucial. The algorithm can be generalized to arbitrary source and arbitrary code alphabet sizes. Its implementation is discussed.

R. Ahlswede and A. Kaspi

On binary state symmetric Markov channels

We study the structure of the transition matrix of binary-input binary-output Markov channels that are symmetric in the sense that the transition probability is invariant under simultaneous complementation of the input, the output and the state of the channel.

Using the structure of the transition matrix, we give bounds on the capacity of the "trap door" channel and show that the zero error capacity of this channel is 0.5.

A multi-terminal problem that arises from the "trap door" channel is presented, and it is shown that one of the extreme points in its achievable region is $(0,\log(0.5(1+\sqrt{5}))$, where the second term results from the limit of the Fibonacci sequence.

K. Kobayashi

The capacity of the permuting relay channel

Blackwell's trap door channel is a nice example of finite state channels. Its deterministic versions, that is, permuting channels, have been studied by Ahlswede and Kaspi (1984) in a multi-terminal information-theoretic frame work. They determined the capacities of permuting jammer channels and relay channels for some special cases. In this talk, we completely solve the capacity problem for permuting relay channels. More specifically, when α is the cardinality of alphabet, and β is the number of available stock locations in channel, the capacity $C_R(\alpha,\beta)$ of the permuting relay channel is given by $\log \lambda$, where λ denotes the maximum eigenvalue of a matrix Q derived from the state transition mechanism associated with the channel.

T. Helleseth

Optimal linear codes

An $[n,k,d]$ code C is a k-dimensional subspace of $GF(2)^n$ such that the minimum Hamming distance between the codewords of C equals d. Further, $n(k,d)$ is defined as the smallest integer n such that an $[n,k,d]$ code exists.

For $k \leq 7$, $n(k,d)$ has been determined by H. van Tilborg.[7]
For $k = 8$ it is known that $n(8,d) = \sum_{i=0} \lceil d/2^i \rceil$ for all $d \geq 131$, where $\lceil x \rceil$ is the smallest integer $\leq x$.
In a recent paper Dodunekov and Manev have determined or given the best known bounds on $n(8,d)$ for $3 \leq d \leq 130$.

We improve these bounds as follows:

$$n(8,16) \geq 37\,,\ n(8,30) \leq 65\,,\ n(8,32) = 68\,,\ n(8,34) \leq 75$$
$$n(8,36) \leq 78\,,\ n(8,40) \geq 84\,,\ n(8,42) \leq 90\,,\ n(8,44) \in [92,93]$$
$$n(8,52) \leq 109\,,\ n(8,58) \geq 120\,,\ n(8,60) \geq 123\,.$$

E.C. van der Meulen

Reliable transmission of two arbitrarily correlated information sources over a discrete memoryless asymmetric multiple-access channel

A discrete memoryless asymmetric multiple-access channel with two encoders is a "two sender - one receiver" multiple-access communication situation whereby messages of one source are encoded by both encoders, whereas the messages of another message set are encoded by only one of them. In this contribution necessary and sufficient conditions are given for the transmission of two arbitrarily correlated sources over such a discrete memoryless asymmetric multiple-access channel. The result shows that in this situation the so-called separation principle holds. An example is given illustrating the theorem. Furthermore it is demonstrated that the same conditions continue to hold when feedback is available to one or both of the encoders. This research builds forth on the work by Cover, El Gamal, and Salehi (1980), Dueck (1981), and Ahlswede and Han (1983). In concreto, the theorem reads as follows:

a. A correlated source $(\mathcal{U}\times\mathcal{V},p(u,v))$ can be transmitted reliably over a d.m. AMAC K_{21} if there exists a prob. distrib. $P(x_1,x_2)$ such that

$$H(U|V) < I(X_1;Y|X_2)$$
$$H(U,V) < I(X_1,X_2;Y)$$

where $P(x_1,x_2,y) = P(x_1,x_2)\,P(y|x_1,x_2)$.

b. Conversely, if a correlated source pair $(\mathcal{U}\times\mathcal{V},p(u,v))$ can be transmitted reliably over a given d.m. AMAC $K_{21}=(\mathcal{X}_1\times\mathcal{X}_2,P(y|x_1,x_2),\mathcal{Y})$, then the following inequalities must be true for some prob. distrib. $P(x_1,x_2)$:

$$H(U|V) \leq I(X_1;Y|X_2)$$
$$H(U,V) \leq I(X_1,X_2;Y).$$

H. Niederreiter

Applications of algebraic coding theory to cryptography

Various ways of using algebraic coding theory in the design of crypto-systems are discussed. In particular, we show how knapsack-type crypto-systems with a high information rate can be obtained from suitable codes.

G.J. Simmons

Information theory and the authentication of digital messages

A model for the authentication of digital messages as a zero-sum two person game was used to derive a channel bound for the authentication channel, in which the value of the game is the probability, P_d, that an opponent can deceive the receiver. The channel bound can be expressed in the form

$$\text{Log}_2 P_d \geq -(H(M)-H(S)-H(M|ES)) \qquad (1)$$

where $H(S)$ is the source entropy, $H(E)$ is the entropy of the strategy with which the transmitter and receiver choose an encoding rule (source states to messages), $H(M)$ is the induced entropy of the messages and $H(M|ES)$ is the average uncertainty of the message if the source state and encoding rule are known. If equality holds in (1), the authentication system is said to be perfect in the sense that all of the information in a message is used to either communicate the state of the source to the receiver, or to confound the opponent. It was shown that affine resolvable designs - and a new class of affine "weakly" resolvable designs - give perfect authentication systems with $P_d = \frac{k}{b}$.

G.F.M. Beenker

Binary transmission codes with higher order spectral zeros at zero frequency

A method is presented for designing binary transmission codes in such a way that both the power spectral density function and its low order derivations vanish at zero frequency.

Codes are called of k-th order zero disparity if all code words $\underline{x} = (x_1,\ldots,x_n)$, $x_i \in \{-1,1\}$, satisfy $\sum_{i=1}^{n} i^k x_i = 0$ for $k \in \{0,1,\ldots,K\}$. The power spectral density function and its first $2k + 1$ derivatives of a k-th order zero disparity code can easily be shown to vanish at zero frequency.

The maximum number of codewords of a k-th order zero disparity code of length n is determined as a coefficient of a generating function in two variables, for all $n \in \mathbb{N}$. For $k = 1$ a lower as well as an upperbound for this number is derived.

It is shown that the minimum distance of a k-th order zero disparity code is at least $2k + 2$.

R. Ahlswede and G. Dueck

Identification via channels

Our main discovery is that $N = \exp\{\exp\{R \cdot n\}\}$ (double exponentially many!) objects can be identified in blocklength n with arbitrarily small error probability via a discrete memoryless channel (DMC), if randomisation can be used for the encoding procedure.

Moreover, we present a novel (second order) Coding Theorem, which determines the second order identification capacity of the DMC as a function of its transmission matrix. Surprisingly this identification capacity is a well-known quantity: it equals Shannon's transmission capacity for the DMC.
The impact of this result for identification problems in computers, psychology or other areas remains to be explored.

J. Körner

Graph entropy and its relevance to combinatorics

The graph G is covered by the union of the graphs, G_i, $i = 1,2,\ldots,t$ if all these graphs have the same vertex set and every edge of G is contained in at least one of the G_i's. In a graph covering problem one is given a graph G and a family of graphs $\mathcal{G}$. One then asks for the minimum number of graphs G_i, $i = 1,2,\ldots,t$ such that G_i is in $\mathcal{G}$ and the union of the G_i's covers G. In order to get lower bounds on t one can use a functional which is sub-additive with respect to the union of graphs. Such a functional is graph entropy, introduced by Körner, 1973. Given a distribution P on the vertex set of G, the entropy $H(G,P)$ is

$$\min_{X \in Y \in \mathcal{V}(G),\ P_X = P} I(X \wedge Y)$$

where $I(X \wedge Y)$ is natural information and $\mathcal{V}(G)$ is the family of independent sets of G. Graph entropy and its natural generalization, hypergraph entropy were used by Körner and Marton to improve on the Fredman-Komlós bounds for the minimum number of perfect (b,k)-hash functions. The analysis of the method leads to an interesting conjecture on perfect graphs that is proved here for bipartite graphs.

K. Marton and J. Körner

Random access communication and graph entropy

Conflict resolution in random access communication raises the following probabilistic problem. Let $U_1,\ldots,U_k$ be independent random variables uniformly distributed in the unit interval $[0,1]$. A k-partition A of $[0,1]$ (i.e. a partition into k atoms) separates the points $U_1,\ldots,U_k$ if each atom of A contains exactly one of the U_i. For k-partitions $A_1,\ldots,A_n$, let $P_{A_1,\ldots,A_n}(k)$

be the probability of the event that at least one of the A_j's separates $U_1,\ldots,U_k$. What is the maximum of these probabilities, if $A_1,\ldots,A_n$ vary? Hajek's conjecture (supported by the Van der Waerden-Falikman-Egorychev theorem) was:

$$\min[1-P_{A_1,\ldots,A_n}(k)] = (1-\frac{k!}{k^k})^n \ .$$

We disprove this by showing $\min[1-P_{A_1,\ldots,A_n}(3)] \leq \frac{25}{81}$, and prove the bounds

$$1-P_{A_1,\ldots,A_n}(k) \geq 2^{-n\,k!/k^{k-1}} \ .$$

This is achieved by a new technique for lower bounding the number of graphs of a given structure needed to cover all edges of a given graph. This technique, developed by J. Körner, is based on the subadditivity of graph entropy - a functional on graphs.

C. Heegard

On the spectrum of (d,k) codes

In this talk we present a simple method to obtain the spectrum of a (d,k) code. A (d,k) code describes a set of binary waveforms, $\omega(t) \in \{-1,+1\}$, that have a minimum ($T_{min}=d+1$) and maximum ($T_{max}=k+1$) length of time between transitions (note: all transitions in $\omega(t)$ occur at integer times). The waveform $\omega(t)$ is described by several sequences: the level sequence $z_0 = \omega(0^+)$, $z_1 = \omega(1^+)$, $z_2 = \omega(2^+),\ldots$; the transition sequence $x_1 = (z_1-z_0)/2, x_2 = (z_2-z_1)/2,\ldots$ (note: $x_j \in \{-1,0,+1\}$); the state sequence

$$s_j = \begin{cases} 0 & x_j \neq 0 \\ s_{j-1}+1 & x_j = 0 \end{cases}$$ and the runlength sequence

$T_1,T_2,\ldots$ (where $T_i=s_{j-1}+1$ if $x_j\neq 0$). As random processes, the entropies are related by $H(Z) = H(X) = H(S) = H(T)/E(T)$.

Theorem: For i.i.d. runlengths (i.e. the state sequence is a Markov chain)

$$S_x(D) \equiv \sum_{j=-\infty}^{\infty} Ex_j x_0 D^j = \pi_0 \frac{1-g(D)g(D^{-1})}{(1+g(D)(1+g(D^{-1})} \quad \text{where}$$

$$g(D) = \sum_{j=d+1}^{k+1} P_r(T_1=j)D^j \quad \text{and} \quad \pi_0 = P_r(s_0=0) = P_r(x_j\neq 0) = \frac{1}{E(T)} = \frac{1}{g'(D)}\Big|_{D=1}.$$

A simple derivation of this theorem is given (note: $S_Z(D) = 4S_x(D)/(1-D)(1-D^{-1})$). The method is then extended to find the spectrum of a popular (d,k) known as MFM (a code that satisfies d=1, k=3).

Z. Zhang and Toby Berger

Multiple description source coding in the excess rate situation

The source data $\{X_i\}_{i=1}^{\infty}$ is encoded into two code f_1 and f_2 at rates r_1 and r_2 respectively. These two codes are sent to three decoders. Two of these decoders observe f_1 and f_2 respectively whereas the third one observes both of them. They recover the source messages with average distortions d_1, d_2, and d_0. Let R be the region of all of the achievable quintuples (r_1,r_2,d_0,d_1,d_2) in the usual Shannon's sence. In the no excess rate situation defined by $r_1 + r_2 = R(d_0)$, R has been determined. In the excess rate situation defined by $r_1 + r_2 > R(d_0)$, the problem seems extremly difficult. A special case of this situation is that $r_1 = R(d_1)$, $r_2 = R(d_2)$. We obtain both an inner bound and an outer bound of R in this case. The gap between them is very small. On basis of this fact, we conjecture that the following upper bound is tight in this case.

Theorem: (r_1,r_2,d_0,d_1,d_2) is acievable if there exist r.v's X_1, X_2, U, jointly distributed with generic r.v. X such that the following conditions are satisfied.

1. $\exists$. S_1,S_2,S_0 s.t.
$Ed(X;S_i(X_i,U)) \leq d_i \quad i = 1,2,$
$Ed(X;S_0(X_1,X_2,U)) \leq d_0;$

2. $r_1 + r_2 \geq 2I(X;U) + I(X_1;X_2|U) + I(X;X_1,X_2|U),$

3. $r_i \geq I(X;X_i,U), \quad i = 1,2.$

V.V. Zyablov, V.A. Zinoviev, S.A. Portnoy

Decoding of generalized concatenated codes and demodulation

Let A,B,C correspond inner, outer and generalized concatenated (GC) code of order m. That means that we use m inner and m outer codes to obtain GC-code C. The i-th outer code B_i, $i = 1,\ldots,m$, over the alphabet of size q_i and with power $N_{b,i}$ can be selected independently of other outer codes only with the same length n_b. The inner code must be the system of nested codes of length n_a. Let A_i be i-th inner code. Then A_1 is partition of q_1 codes $A_2(i)$, $i = 0,1,\ldots,q_1-1$, which have the same parameters. Every code $A_2(i)$ is partition of q_2 codes $A_3(i_1,i_2)$ and so on... Let values of symbol of inner codes are selected from space E with Hamming d_H or Euclidian d_E metric, where d_E means square of Euclidian distance. We require also that for every j, $j = 1,\ldots,m-1$, there exists an automorphism $S_j: E^{n_a} \to E^{n_a}$ such that $S_j(A_j(0,\ldots,0,i_{j-1})) = A_j(0,\ldots,0,0)$, $i_{j-1} = 0,1,\ldots,q_{j-1}-1$, and for every $x,y \in E^{n_a}$ $d(x,y) = d(S_j(x),S_j(y))$.

Let $d_{a,i}$ and $d_{b,i}$ be the minimum distances of A_i and B_i correspondingly, where $d_{a,i}$ can be d_H or d_E. Then GC-code has parameters: $n = n_a n_b$, $d \geq \min\limits_{1\leq i\leq m} \{d_{a,i} d_{b,i}\}$, $N = N_{b,1} \cdots N_{b,m}$.

The decoding algorithm consists from m steps Ψ_i, $i = 1,\ldots,m$. We want that i-th step Ψ_i don't depend of result of decoding Ψ_j, $j < i$. For this we want to deal only with the i-th inner code $A_i(0,\ldots,0)$ and outer code B_i. After the decoding Ψ_i we'll have some word $b^{(i)} = (b_1^{(i)},\ldots,b_{n_b}^{(i)})$ of the code B_i and therefore n_b codes $A_{i+1}(0,\ldots,0,b_\rho^{(i)})$, $\rho = 1,\ldots,n_b$. Then using the automorphism S_{i+1} we transform the code $A_{i+1}(0,\ldots,0,b_\rho^{(i)})$ to code $A_{i+1}(0,\ldots,0,0)$ for every ρ. Exact description of the step Ψ_i one can find in paper (Dumer I.I., Zinoviev V.A., Zyablov V.V., Problems of Control and Information Theory, 1983). Such decoding algorithm overally realize the minimum distance of GC-code and has complexity of decoding, which grows with the length of code $n = n_a n_b$ approximatly as n^c, where usually $c = 2$. Applications of this result are interested, when the inner codes are phase or amplitude-phase modulation. In this case we have regular method demodulation and decoding simultaniously (Portnoy S.L., Problem of Inform. Transm., 1985, 21, W3, 14-27).

H.C.A. van Tilborg

Burst identification codes

Consider the vectorspace A of all binary $n_1 \times n_2$ arrays. A $b_1 \times b_2$ burst in A is an $n_1 \times n_2$ array, all of whose non zero elements are confined to a $b_1 \times b_2$ subrectangle. A linear code (subspace) C is said to be a $b_1 \times b_2$-burst identification code, if the pattern of any single $b_1 \times b_2$ burst can be identified. Together with burst location codes, one can correct the burst.
Let r be the minimal redundancy of a linear, $b_1 \times b_2$ burst identification code. Then it can be shown that $r \geq 2b_1b_2-2$. An explicit construction (+ decoding algorithm) is given of a $b_1 \times b_2$-burst identification code with redundancy $r = 2b_1b_2$.

G. Cohen

An application of combinatorial group theory to coding

We consider two problems in combinatorial group theory and give applications to coding. Let $(G,+)$ be a finite abelian group.

Problem 1. Determine $s(G)$, defined as the smallest integer such that $\forall S, S \subset G, |S| \geq s(G) \Rightarrow S$ contains a subset with zero sum.

Olson has solved it for p-groups. This was used by Alon to prove the following conjecture for m a power of two.

Conjecture (Ito). Every binary linear $[4m,2m+1]$ code contains a vector of weight $2m$.

Problem 2. Determine $c(G,t)$, defined as the smallest integer such that if S is a generating subset of G with cardinality $c(G,t)$, every non zero element of G can be expressed as a sum of at most t elements in S.
We consider the case $G = (\mathbb{Z}/2\mathbb{Z})^r$, which is related to coding, and prove

Proposition $c((\mathbb{Z}/2\mathbb{Z})^r,t) \leq \frac{2r}{t}$, for t a power of two.

Problem 3. Is the Proposition true for general t?

Finally, we give an application to coding for reusing write-once memories.

This work was done jointly with G. Zemor.

M.H.M. Costa

Gaussian interference channels

The Gaussian interference channel, introduced by Carleial in 1975, models the communication between average power constrained senders X_1 and X_2 to their respective receivers Y_1 and Y_2 over a shared medium with additive Gaussian noise. The channel inputs and outputs are related by $Y_1 = X_1 + b\,X_2 + Z_1$ and $Y_2 = a\,X_1 + X_2 + Z_2$, where a and b are non-negative interference parameters, and Z_1 and Z_2 are unit variance normally distributed noise terms. The capacity region has been obtained when interference is strong (i.e., $a \geq 1$ and $b \geq 1$), but is yet to be established when one of the interference parameters is in the open unit interval. We examine the simpler model of the Z-Gaussian interference channel, where one of the interference parameters is zero. A signaling scheme is proposed that combines the known techniques of superposition coding and time-sharing (or frequency-sharing). This scheme is optimal within the restricted class of Gaussian signaling techniques. We motivate the conjecture that this scheme yields the capacity region of the Z-Gaussian interference channel. If true, this conjecture leads to an improved outer bound of the capacity region of the general Gaussian interference channel (with arbitrary parameters).

M.R. Best

A Markov source model for a convolutional coding scheme

A convolutional coding scheme with maximum likelihood decoding over a discrete memoryless channel can be modelled as a Markov source. Using this model, the statistical behaviour of the errors can be analysed exactly. In effect, not only the bit and event error probability, but also the burst and gap length distribution can be computed. Moreover, for a (suboptimum) Viterbi decoder with a finite decoding delay the dependence of the error statistics on that delay can be found. This generalizes earlier results of Schalkwijk, Post and Aarts.

T.S. Han

Hypothesis testing with multiterminal data compression

The multiterminal hypothesis testing $H:XY$ against $\bar{H}:\bar{X}\bar{Y}$ is considered where $X^n(\bar{X}^n)$ and $Y^n(\bar{Y}^n)$ are separately encoded at rates R_1, R_2, respectively. The problem here is to determine the minimum β_n of the second kind of error probability, under the condition that the first kind of error probability $\alpha_n \leq \varepsilon$ for a prescribed $0 < \varepsilon < 1$. We are concerned with the asymptotic behaviour of β_n, so define $\theta(R_1,R_2,\varepsilon) = \lim_{n\to\infty} \inf(-\frac{1}{n} \log \beta_n)$, which is called the power exponent. We established a good lower bound $\theta_L(R_1,R_2)$ on this power exponent and revealed several interesting properties. The $\theta_L(R_1,R_2)$ is tighter than that of Ahlswede and Csiszár, who first set up the multiterminal framework for hypothesis testing. Main arguments are devoted to the case $R_2 = +\infty$ (full side information case). It is conjectured that $\theta_L(R_1,R_2)$ is tight at least in case of $R_2 = +\infty$.

Also, we give the complete solution to the case only with one bit compression.

E. von Collani

An entropic concept in Statistical Quality Control

Consider the following problem which arises in Statistical Quality Control: A lot of size N is to be inspected by means of a single sampling plan (n,c) with $0 \leq c < n \leq N$, i.e. a random sample of size n is taken and if the number of nonconforming items in the sample is less than or equal to the acceptance number c, the lot is accepted otherwise rejected. The problem is to determine an appropriate sampling plan (n,c) given a linear cost model.

There are three sampling schemes to solve this problem and which may be classified according to their assumptions about the probability distribution of the number of nonconforming items M in a lot:

1. Bayes-plans, assuming complete knowledge about the probability distribution of M
2. Minimax-plans, assuming that there is no knowledge at all about the probability distribution and

3. α-Minimax-plans which assume that one point (for the break-even quality) of the distribution function of M is known.

To be able to compare the different concepts and to find the relevant informations about the probability distribution, an entropic sampling plan is defined applying the principle of Maximum Entropy.

K. Marton

Weak asymptotic isomorphy of correlated sources

Isomorphy problems for correlated sources were raised in ergodic theory (Thouvenot 1975), but the interest in them is also motivated by multi-terminal information theory. A DMSC (discrete memoryless stationary correlated) source is an i.i.d. sequence of random pairs with values in a finite set. Here we consider weak asymptotic isomorphy of DMSC sources. Two DMSC sources $\{(X_i,Z_i)\}_{i=-\infty}^{\infty}$, $\{(X'_i,Z'_i)\}_{i=-\infty}^{\infty}$ are asymptotically isomorphic in the weak sense if for $\varepsilon > 0$ and large enough n, there exists a joint distribution of the n-length outputs of the two sources, $\mathrm{dist}(X^n,Z^n,X'^n,Z'^n)$ satisfying

$$\frac{1}{n}H(X^n|X'^n) < \varepsilon\,,\ \frac{1}{n}H(X'^n|X^n) < \varepsilon\,,\ \frac{1}{n}H(Z^n|Z'^n) < \varepsilon\,,\ \frac{1}{n}H(Z'^n|Z^n) < \varepsilon\,.$$

We prove that some spectral properties of the distribution $\mathrm{dist}(X_1,Z_1)$ are invariant for weak asymptotic isomorphy, and these properties wholly determine the distribution in many cases.

C.P. Schnoor

An efficient identification and signature scheme

A. Shamir proposed the following interactive authentication scheme.
Let n be a composite number that is hard to factor.
Let Alice have public key $k_A \bmod n$ and private key $\sqrt{k_A} \bmod n$.
If Alice identifies herself to Bob she picks a random $r \pmod n$, sends $t := r^2 \bmod n$ to Bob and lets Bob choose to see either $\sqrt{t}$ or $\sqrt{tk_A} \bmod n$. Bob decides at random. If Alice and Bob used independent random numbers then Bob is safe against forgery and Alice does not reveal any information on $\sqrt{k_A} \bmod n$ to Bob.

We extend this scheme so that the exchanged data can be used

to convince a third party, e.g. a judge.
For this Alice and Bob generate pseudorandom number $R_A = R(\sqrt{k}_A \bmod n, \text{rand})$, $R_B = R(\sqrt{k}_B \bmod n, \text{rand})$ that can lateron be controled by a trusted authority that knows $\sqrt{k}_A$ and $\sqrt{k}_B$.

T. Ericson

1. Asymptotic properties of equal weight codes
2. Disjunctive codes and protocol sequences

Asymptotic properties of equal weight codes (Thomas Ericson)

Let $EW(n,w,c,T)$ denote the (possibly empty) family of binary codes of length n, weight w, maximum correlation c, and size T. Define

$$T(n,w,c) \triangleq \max\{T:EW(n,w,c,T)\neq\phi\}.$$

We will discuss various asymptotic properties of this quantity as $n \to \infty$; especially the case when $w = \lfloor n\nu \rfloor$; $c = \lfloor n\kappa\nu \rfloor$ for some constants ν,κ.

Disjunctive codes and protocol sequences (Thomas Ericson, Victor Zinoviev)

Kautz and Singleton introduced Superimposed codes in 1964 [1], these same codes were later studied under the name of disjunctive code by Dyachkov-Rykov [2] and others. Lately the connection with protocol sequences has been observed [3]. In this context we will present some new results; in particular an existance bound based on the Varshamov Gilbert bound.

[1] Kautz, W.H. and Singleton, R.C., "Nonrandom Binary Superimpose Codes", IEEE Trans. on Inf. Th.

[2] Dyachkov, A.G. and Rykov, V.V., "Bounds on the Length of Disjuctive Codes", translated from Problemy Peredachi Informatsii, Vol. 18, No. 3, pp. 7-13, July-September, 1982.

[3] Nguyen Quang A, Györfi Laszlo, Massey, James L., "Performances of Protocol sets for Collision Channel without Feedback.

T. Ericson, V. Zinoviev

Asymptotic properties of equal weight codes

An equal weight code is a binary code such that all codewords have the same weight. Denote by $T(n,\omega,c)$ the maximal possible size of such a code, when the length is n, the common weight is ω, and the maximal correlation between codewords is c. We are interested in the asymptotic behaviour of $T(n,\lfloor \nu n \rfloor,\lfloor \nu x n \rfloor)$ as $n \to \infty$, where $\nu \triangleq \frac{\omega}{n}$ are held fixed. Exponential increase of T is obtained if and only if $x > \nu$. The exponent is easily lower bounded by the Gilbert bound. By combining a construction by Kautz-Singleton with a recent result by Tsfasman-Vladut-Zink we obtain an improvement of this bound in a certain range $x_1 < x < x_2$, provided $\nu = \frac{1}{p^{2s}}$, p is a prime, $s = 1,2,\ldots,$ and $p \geq 11$.

The simplest upper bound (for the size of an equal weight code) is Johnson bound: $T(n,\omega,c) \leq \binom{n}{c+1} / \binom{\omega}{c+1}$. For certain values of the parameters (n,ω,c) this bound is satisfied with equality. The corresponding code is equivalent to Steiner system $S(n,\omega,c+1)$. There are a few infinite families of Steiner systems, including cyclic ones. They provide optimal protocols for multi-user channels without feedback both in the synchronious case (Steiner systems) and the asynchronious case (cyclic Steiner system). There are also special constructions of the cyclic Steiner systems $S(n,3,2)$, which for $n \equiv 1 \pmod 6$ give optimal solutions for self-orthogonal convolutional codes.

W.B. Müller

On commutative groups of polynomial functions and their applications in cryptography

During the last years the discrete exponentiation $x \to x^k$ has been used as one-way function in the Diffie-Hellman key distribution, in Shamir's three-pass algorithm and in the RSA-public key cryptosystem. Until recently, the computation of discrete logarithms, the inverse function of the discrete exponentiation, was believed to be a very hard problem. But recently progress in computing discrete logarithms has been made, especially in Galois

fields of characteristic 2. In order to protect the above mentioned schemes against attacks by these recent algorithms one can replace the discrete exponentiation $x \to x^k$ by more sophisticated polynomial functions $x \to f(x)$, which also commute with respect to composition. It is shown that the so-caled Dickson-polynomial functions $x \to g_k(1,x)$ and $x \to g_k(-1,x)$ can be used as cipher functions (cf. Müller, W.B. and R. Nöbauer: Cryptanalysis of the Dickson-scheme. To appear in Proc. Eurocrypt 85, Lecture Notes in Computer Science).

Another group pf polynomial functions on $\mathbb{Z}/(n)$ can be obtained from polynomials of the form $l^{-1} \cdot x^k \cdot l$ with $l = ax + b \in \mathbb{R}[x]$, $a \neq 0$. It can be proved that $l^{-1} \cdot x^k \cdot l$ with $k \in 2\mathbb{N}+1$ is a polynomial over $\mathbb{Z}$ iff $a^2, ab, b^2 \in \mathbb{Z}$ and $b^3-b \in a\mathbb{Z}$. Furthermore, the function $x \to \frac{x}{a} \cdot x^k \cdot ax$ with $a \neq 0$, $a^2 \in \mathbb{Z}$ is a permutation of $\mathbb{Z}/(n)$ iff $(k,\varphi(n)) = 1$ and $(a^2,n) = 1$. At last, all permutations of $\mathbb{Z}/(n)$ of this form with only one fixed point are described. (If $n = p_1 p_2 \ldots p_r$, any permutation of $\mathbb{Z}/(n)$ induced by polynomials x^k has at least 3^r fixed points.)

P. Nyffeler

Source properties of sequences over local rings

The talk concernes the question: what can be saved, when generalizing periodic (or recurrence) sequences over finite fields to sequences over local rings, especially over $\mathbb{Z}_{p^r}$ or Galois rings $GR(p^r,K)$: Over finite fields, the shift registers are canonical forms of finite-state machines, as representatives of companion matrices. Over local rings, shift registers modulo a nilpotent ideal play a similar role. The analysis of sequences can be done by an algorithm similar to the Berlekamp-Massey algorithm over $\mathbb{Z}_{p^r}$ and the synthesis of new sequences of higher complexity by "root combinations" is possible.

A. Tietäväinen

Upper bounds for codes

Let $A(n,d)$ be the maximum number of code words in a binary code of length n and minimum distance at least d. We derive two asymptotical upper bounds for the number $A(2d+j,d)$ when $d \to \infty$ and j is paritive and small, show that these bounds are in a sense best possible, and consider some open problems, generalizations and modifications. We also show how the second McEliece-Rodemich-Rumsey-Welch bound has been generalized to the nonbinary case.

Ph. Piret

Bounds for codes over the unit circle

Let C be a code of length n and rate R over $A(Q) = \{\exp(2\pi ir/Q): r = 0,1,\ldots,Q-1\}$, and let $d(C)$ be the mimimum Euclidean distance of C. For large n, lower and upper bounds are obtained in parametric form on the achievable pairs (R,δ), which $\delta = d^2(C)/n$. For $Q \to \infty$ they are shown to be expressible in terms of modified Bessel function of the first kind. The upper bound is compared with the Kabatyanskii-Levenshtein bound that holds for less restrictive alphabets. For $Q \to \infty$, it is stronger than the K-L bound for $\delta \leq 0.93$.

J.L. Massey

Sequences with perfect linear complexity profiles

The linear complexity, $L(s^n)$, of a sequence $s^n = (S_0,S_1,\ldots,S_{n-1})$, $s_i \in F$ (an arbitrary field) is the smallest nonnegative integer L such that there exist $c_1,c_2,\ldots,c_L$ in F satisfying

$$s_j + c_1 s_{j-1} + \ldots + c_L s_{j-L} = 0, \qquad L \leq j < n.$$

A binary (i.e., $F = GF(2)$) sequence s^n is said to have a perfect linear complexity profile when

$$L(s^m) = \left\lfloor \frac{m+1}{2} \right\rfloor, \quad 1 \leq m \leq n.$$

The following result was obtained with (and mainly by) the author's doctoral student, M.-Z. Wang:

Theorem: The binary sequence s^n has a perfect linear complexity profile if and only if $s_0 = 1$ and $s_{2i} + s_{2i-1} + s_{i-1} = 0$ for $1 \leq i < \lceil \frac{n}{2} \rceil$.

R. Ahlswede

On code pairs with specified Hamming distances

For a function $f: X \times Y \to Z$ with X, Y, Z finite $C(f)$ is the minimal number of bits two persons, one knowing x and the other y, have to exchange in the worst case so that both can evaluate $f(x,y)$. Yao proved

$$C(f) \geq \log D(f),$$

where $D(f)$ is the minimal size of a partition of $X \times Y$ into rectangles $S \times T (S \subset X, T \subset Y)$, on which f is constant. Those rectangles are called monochromatic.

The determination of D or even the size of the largest monochromatic rectangle $M_z(f)$ in $\{(x,y) \in X \times Y : f(x,y) = z\}$ leads for many functions to new extremal problems, in particular for product spaces $X = Y = \{1, \ldots, \alpha\}^n$.

We consider here Π_n^α, the parity of the Hamming distance d, which is defined by

$$\Pi_n^\alpha(x^n, y^n) = \psi(d(x^n, y^n)), \quad \psi(n) = \begin{cases} 0, & n \text{ even} \\ 1, & n \text{ odd} \end{cases}.$$

Theorem 1 For $n \in \mathbb{N}$, $\bar{\alpha} = \lfloor \frac{\alpha}{2} \rfloor \lceil \frac{\alpha}{2} \rceil$, and $i = 0, 1$.

(a) $M_i(\Pi_n^\alpha) = \begin{cases} 4^{n-1}, & \alpha = 2 \\ \bar{\alpha}^n, & \alpha \geq 4 \end{cases}$ and $\psi(n) = i$

(b) $\bar{\alpha}^{n-1} \leq M_i(\Pi_n^\alpha) < \bar{\alpha}^n$, $\alpha \geq 4$ and $\psi(n) \neq i$.

Corollary $C(\Pi_n^4) = D(\Pi_n^4) = 2n + 1$.

Related results: A rectangle $A\times B$; $A,B \subset \{1,\dots,\alpha\}^n$; has one-sided equiparity, if $\Pi_n^\alpha(a,b) = \Pi_n^\alpha(a,b')$ for every $a \in A$ and all $b,b' \in B$.

For the maximal cardinality $\vec{M}(n,\alpha)$ of such rectangles we have

Theorem 2 For $n \in \mathbb{N}$ $\vec{M}(n,\alpha) = \begin{cases} 2\cdot 4^{n-1} & , \alpha = 2 \\ (2^n+1)2^{n-1} & , \alpha = 3 \\ \alpha^n & , \alpha \geq 4 \end{cases}$.

The set $A \subset \{1,2,\dots,\alpha\}^n$ has i-parity (i=0,1), if $\Pi(a,a') = i$ for $a,a' \in A$ with $a \neq a'$.

Theorem 3 For $n \in \mathbb{N}$

$$\max\{|A| : A \subset \{1,2,\dots,\alpha\}^n \text{ has 0-parity}\} = \begin{cases} 2^{n-1} & , \alpha = 2 \\ 2^{n-1}+1-\psi(n) & , \alpha = 3 \\ \alpha^{\lfloor n/2 \rfloor} & , \alpha \geq 4 \end{cases} .$$

The corresponding problem for 1-parity sets is unsolved.

More problems, conjectures and also results in distributive computing and multi-user source coding are presented in a paper with the same title, which has been submitted to the European J. of Combinatorics.

J.H. van Lint

Duadic Codes

Duadic codes over GF(2) were introduced by Leon, Masley and Pless in 1984. We present results on these codes and generalisations to GF(q) which were obtained by M.H.M. Smid (1986) in his master's thesis (T.H. Eindhoven). Let n be odd, $(n,q) = 1$. If S_1 and S_2 are unions of cyclotomic cosets mod n, $S_1 \cap S_2 = \emptyset$, $S_1 \cup S_2 = \{1,2,\dots,n-1\}$ and if the permutation $\mu_a : x \to ax$ interchanges S_1 and S_2 than (μ_a, S_1, S_2) is called a splitting mod n. A duadic code C_i (resp. C_i') is the cyclic code with generator $g_i(x) := \prod_{j \in S_i} (x-\alpha^j)$ (resp. $(x-1)\, g_i(x)$).

(Remark: For $q = 2$ this is not the definition given by Leon, Masley and Pless but the definitions are equivalent.) The QR codes, some special RS and GRM codes are duadic codes (all with μ_{-1}).

Theorem: If C is cyclic and $\bar{C}$ is self-dual, then C is duadic with splitting given by μ_{-1}.

Theorem: Let $n = p_1^{m_1},\ldots,p_k^{m_k}$. A splitting mod n exists $\Leftrightarrow$ q is a square mod p_i for all i. For all binary duadic codes of length <127 the minimum distance was calculated using the "new bound". Several Theorems on duadic codes are given, showing that many of them have low minimum distance.

Berichterstatter: Ingo Althöfer (Bielefeld)

Tagungsteilenehmer

Prof. Dr. R. Ahlswede
Mathematische Fakultät
Universität Bielefeld
Universitätsstr. 1

4800 B i e l e f e l d 1

Dipl.-Math. Ingo Althöfer
Mathematische Fakultät
Universität Bielefeld
Universitätsstr. 1

4800 B i e l e f e l d 1

Prof. Dr. E. F. Assmus, Jr.
Mathematics Department
Lehigh University
Christmas-Saucon Hall 14

B e t h l e h e m , PA 18015
U S A

Dr. G. F. M. Beenker
Philips Research Laboratories
PO Box 80.000

NL-5600 JA E i n d h o v e n
Niederlande

Dr. M. R. Best
Twente University of Technology
Dept. of Electrical Engineering
P.O.Box 127

NL-7500 AE E n s c h e d e
Niederlande

Prof. Dr. Th. Beth
Institut für Informatik
Fritz-Erler-Str. 1-3

7500 K a r l s r u h e 1

Dr. R. Calderbank
AT&T Bell Laboratories
Room 2C-363
600 Mountain Avenue

Murray Hill, NJ 07974
U S A

Gérard C o h e n
22 rue Dussoubs

F-75002 P a r i s
Frankreich

Dr. E. von Collani
Institut für Angewandte
Mathematik und Statistik
Universität Würzburg
Sanderring 2

8700 W ü r z b u r g

Dr. M. H. M. Costa
Department Wiskunde
Katholieke Universiteit
Celestijnenlaan 200 B

B-3030 L e u v e n
Belgien

Prof. Dr. I. Csiszar
Hungarian Academy of Sciences
Department of Mathematics
Reáltanoda u. 13-15

H-1053 B u d a p e s t V
Ungarn

Prof. Dr. G. Dueck
Fakultät für Mathematik
Universität Bielefeld
Universitätsstr. 1

4800 B i e l e f e l d 1

Prof. Dr. Th. Ericson
Division of Data Transmission
Dept. of Electrical Engineering
Linköping University
S-581 83 L i n k ö p i n g
Schweden

Prof. Dr. Te Sun H a n
Dept. of Information Systems
School of Business Administrat.
Senshu University
Higashimita 2-1-1, Tama-ku
Kawasaki-Shi
K a n a g a w a 214 / Japan

Prof. Dr. Ch. Heegard
School of Electrical Engineering
Cornell University
I t h a c a , NY 14853
U S A

Prof. Dr. T. Helleseth
Institutt for Informatikk
Universitetet i Bergen
Allégt. 55
N-5000 B e r g e n
Norwegen

Prof. Dr. I. Ingemarsson
Dept. of Electrical Engineering
Linköping Institute of Technolog
S-581 83 L i n k ö p i n g
Schweden

Prof. Dr. A. Kaspi
47 Balfour St.
N a h a r i y a
Israel

Dr. T. Kløve
Institutt for Informatikk
Universitetet i Bergen
Allégt. 55
N-5000 B e r g e n
Norwegen

Prof. Dr. K. Kobayashi
Faculty of Engineering Science
Osaka University
Toyonaka
O s a k a 560
Japan

Prof. Dr. J. Körner
Mathematical Institute of the
Hungarian Academy of Sciences
P.O.B. 127
H-1364 B u d a p e s t
Ungarn

Prof. Dr. J. H. van Lint
Technological University
Dept. of Math. & Computing Sc.
P.O.Box 513
NL-5600 MB E i n d h o v e n
Niederlande

Dr. Katalin Marton
Mathematical Institute of the
Hungarian Academy of Sciences
P.O.B. 127
H-1364 B u d a p e s t
Ungarn

Prof. Dr. J. L. Massey
E. T. H. - Zürich
Institut für Signal- und
Informationsverarbeitung
Gloriastr. 35
CH-8092 Z ü r i c h
Schweiz

Prof. Dr. E. C. van der Meulen
Departement Wiskunde
Katholieke Universiteit Leuven
Celestijnenlaan 200 B
B-3030 L e u v e n
Belgien

Prof. Dr. W. B. Müller
Institut für Mathematik
Universität Klagenfurt
Universitätsstr. 65
A-9010 K l a g e n f u r t
Österreich

Prof. Dr. H. Niederreiter
Kommission für Mathematik
Österreichische Akademie der Wissenschaften
Dr. Ignaz-Seipel-Platz 2
A-1010 W i e n
Österreich

Dr. P. Nyffeler
Bundesamt für Übermittlungstruppen
Sektion Kryptologie
CH-3003 B e r n
Schweiz

Dr. A. M. Odlyzko
AT&T Bell Laboratories
Room 2C-370
600 Mountain Avenue
Murray Hill, NJ 07974
U S A

Dr. Ph. Piret
Philips Research Laboratory
2, avenue van Becelaere
B-1170 B r u s s e l s
Belgien

Dr. K. Post
University of Technology
Dept. of Math. & Computing Sc.
P.O.Box 513
NL-5600 MB E i n d h o v e n
Niederlande

Prof. Dr. J. P. M. Schalkwijk
Dept. of Electrical Engineering
Eindhoven Univ. of Technology
P.O.Box 513
NL-5600 MB E i n d h o v e n
Niederlande

Prof. Dr. C. P. Schnorr
Fachbereich Mathematik
Universität Frankfurt
PSF 11 19 32
Robert-Mayer-Str. 6-10
6000 F r a n k f u r t a.M.

Prof. Dr. G. J. Simmons
Sandia National Laboratories
Applied Mathematics Dept. 1640
A l b u q u e r q u e , NM 87185
U S A

Prof. Dr. A. Tietäväinen
Department of Mathematics
University of Turku
SF-20500 T u r k u 50
Finnland

Prof. Dr. H. C. A. van Tilborg
Dept. of Math. & Comp. Science
Eindhoven Univ. of Technology
P.O.Box 513
NL-5600 MB E i n d h o v e n
Niederlande

Dr. H.-M. Wallmeier
Institut für math. Wirtschafts-
forschung der Universität BI
Universitätsstr. 1

4800 B i e l e f e l d 1

Prof. Dr. Zhe-xian W a n
Institute of Systems Science
Academia Sinica

B e i j i n g 100080

Volksrepublik China

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

NL-5600 MB E i n d h o v e n

Niederlande

Jian-Ping Y e
Universität Bielefeld
Fakultät für Mathematik
Universitätsstr. 1
Postfach 8640

4800 B i e l e f e l d 1

Prof. Dr. Zhen Z h a n g
Universität Bielefeld
Fakultät für Mathematik
Universitätsstr. 1
Postfach 8640

4800 B i e l e f e l d 1

Prof. Dr. V. A. Zinoviev
Institute for Problems and
Information, Transmission of
USSR Academy of Sciences
19, Ermolovoy Str.

101447 M o s c o w GSP 4
U S S R

Angelika Zwacka

SIEMENS AG , ZTI SYS 4
Postfach 83 09 51

8000 M ü n c h e n 83

Prof. Dr. V. Zyablov
Institute for Problems and
Information Transmission of
USSR Academy of Sciences
19, Ermolovoy Str.

101447 M o s c o w GSP 4
U S S R