MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Tagungsbericht 19/2000

Kodierungstheorie

30.4.–6.5.2000

Die Tagung fand statt unter der Leitung von G. van der Geer (Amsterdam), P.V. Kumar (Los Angeles) und H. Stichtenoth (Essen). Insgesamt nahmen 44 Mathematiker(innen) aus 14 Ländern teil, und es wurden 23 Vorträge gehalten. Da die Teilnehmer aus ziemlich verschiedenen Gebiete der Mathematik stammten (von Ingenieuren bis zu algebraischen Geometern), wurde eine Reihe von Tutorials organisiert über neuere Entwicklungen in der Kodierungstheorie, wie zum Beispiel über Kodes auf Graphen, Turbo Kodes, Quantum Kodes und über algebraisch-geometrische Kodes. Dies wurde als wertvoll gesehen. Weitere Themen von Interesse waren Kodes über Ringen, Kurven mit vielen Punkten, Listen-Dekodierung, Zetafunktionen von Kodes und iterative Dekodierung.

Der Programm hat viel Zeit für Diskussionen gelassen, und davon wurde viel profitiert. Es wurde als sehr nützlich empfunden, dass Leute mit sehr verschiedenem Hintergrund die Möglichkeit zum Kontakt hatten. Zum Schluss ein Wort des Dankes für die gute Betreuung durch das Personal und die angenehme Atmosphäre am Forschungsinstitut.

Vortragsauszüge - Abstracts

A.I. BARBERO and C. MUNUERA

The order bound of one-point AG-codes: Weight hierarchy of Hermitian codes

The order bound on the minimum distance of AG codes has been introduced by Feng and Rao and later generalized to all higher weights by Heijnen and Pellikaan. In this talk we show how this bound can be used together with the arithmetical approach to determine the weight hierarchy of many AG-codes. We also show how to manage to compute the order bound in the case of Hermitian codes.

A. BARG

Quantum codes : An introduction

Quantum codes are devised for correction of decoherence errors in entangled states. In this talk I present a general context of quantum information transmission, related to quantum computations, explain the nature of errors on a depolarizing channel, define quantum codes and their distance and the subclass of stabilizer codes. These results are based on the works of R. Calderbank, P. Shor, E. Rains and N. J. A. Sloane. For lack of time, I did not speak of my work on error-detection with quantum codes and exponential bounds on the probability of undetected error.

J. BIERBRAUER

Additive codes: Theory and applications

We describe a new approach to the theory of cyclic codes codes and generalize to the category of additive codes (whose alphabet is a vector space over a ground field). A family of 2-weight codes is derived as an example.

Caps are subsets of projective Galois spaces no three of which are collinear. We construct a family of large cyclic caps by projection from Grassmanian manifolds. The analysis of extendability involves hyperelliptic curves.

Random variables with certain independence properties can be constructed, using linear codes, from weakly biased random variables. The Weil-Carlitz-Uchiyama bound describes the properties of dual-BCH codes in terms of this parameter, the bias. We generalize a construction method due to Alon. et. al. and show how codes over extension fields come into play. Algebraic-geometric codes yield improvements upon the WCU-construction and come close to yielding an asymptotically optimal construction.

P. CHARPIN

On the classification of cosets of $R(1,m)$

By using some techniques introduced by Kasami, we establish a necessary condition for a coset of $R(1,m)$ to have a "high" minimum distance. We next consider Boolean functions and then the coset generated by their corresponding codeword. We are particularly interested by the connection between two cryptographic properties of Boolean functions: nonlinearity and propagation characteristics.

J. F. DILLON

Pseudorandom binary sequences with ideal autocorrelation

Such sequences are equivalent to cyclic difference sets with Singer parameters $(v,k,\lambda) = (2^m-1, 2^{m-1}, 2^{m-2})$. We give a survey of all known such sequences from the pioneering work of Gauss and Galois to the sensational discoveries of the past two years. In particular we show that there are no sporadic such difference sets today—all known such difference sets are explained by a constructive theorem. We also prove the

Theorem. Let $\mathbb{L} = \mathbb{F}_{2^m}$ and for $(k,m) = 1$ define

$$K_k = \{\alpha \in \mathbb{L} : x^{2^k+1} + x = \alpha \quad \text{has a unique solution in} \quad \mathbb{L}\}$$

and $D_k = \mathbb{L} \setminus \{x^d + (x+1)^d + 1 : x \in \mathbb{L}\}, \quad d = 4^k - 2^k + 1.$

Then

$$K_k^{(-1)} = \begin{cases} D_k & \text{if } m \text{ is even} \\ \mathbb{L}^\times \setminus D_k & \text{if } m \text{ is odd.} \end{cases}$$

Corollary. $K_k = \{\alpha \in \mathbb{L}^\times : x^{2^{2k}} + x^{2^k} + \alpha x \quad \text{is 2-to-1 on} \quad \mathbb{L}\}$ is a difference set with Singer parameters.

BCH codes with two zeros

H. DOBBERTIN

While BCH codes with one zero are easily described, it is presently elusive to determine for example, the weight distribution of BCH codes with two zeros. So it is a natural problem to classify all of them which have extremal properties, for instance those which achieve the greatest possible minimum distance, that is 5. This classification problem is equivalent to the classification of all APN (almost perfect nonlinear) power functions on a finite field of characteristic two. We present an overview about the known results and explain a new technique ("multivariate method") which allows to prove new results along this line, as well as to give new proofs for the known cases. The "multivariate"method has however much further reaching applications. For instance, various classes of new permutation polynomials (and new proofs for known permutation polynomials, like the Glynn and Cherowitzo o-polynomials) can be derived.

I. DUURSMA

Self-dual codes and zeta functions

The zeta function of an algebraic curve determines to a large extent, the weight enumerators of linear codes constructed with the curve (through Goppa's construction). The inverse of this relation associates to an arbitrary linear code, not the zeta function of a curve but a function with very similar properties. It is rational, satisfies a functional equation and in some cases an analogue of the Riemann hypothesis. Our observations suggest that a Drinfeld-Vlăduţ type bound holds for self-dual codes:

$$\frac{d}{n} \leq \frac{1}{2} - \frac{1}{2\sqrt{q}}, \quad n \quad \to \infty \ .$$

G. D. FORNEY, JR.

Duality theorems for linear and group codes on graphs

A generalized state realization of the Wiberg type is called normal if symbol variables have degree 1 and state variables have degree 2. A natural graphical model of a normal realization has leaf edges representing symbols, ordinary edges representing states, and vertices representing local constraints. Any Wiberg-type realization can be put into normal form without essential change in the corresponding graph or in its decoding complexity.

Linear or group codes are generated by linear or group realizations. The dual of a normal linear or group realization, appropriately defined, generates the dual code. The dual realization has the same graph topology as the primal realization, replaces symbol and state variables by their character groups, and replaces primal local constraints by their duals. This fundamental result has many applications, including to dual state spaces, dual minimal trellises, duals to Tanner graphs, dual input-output systems, and dual kernel and image representations.

A. GARCIA

On towers of function fields over finite fields

The subject of the talk was a tower over the finite field with p^2 elements ($p \geq 3$ a prime number) attaining the Drinfeld-Vladut bound. The tower is defined recursively by the equation

$$y^2 = \frac{x^2+1}{2x}.$$

The proof involves two new properties of Deuring's polynomial

$$H(X) = \sum_{j=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{j}^2 \cdot X^j \in \mathbb{F}_p[X]:$$

Property A. All roots of $H(X)$ are fourth powers in $\mathbb{F}_{p^2}$.

Property B. The following polynomial identity in $\mathbb{F}_p[X]$ holds

$$H(X^4) = X^{p-1} \cdot H\left(\left(\frac{X^2+1}{2X}\right)^2\right).$$

The subject of this talk is part of a joint paper with H. Stichtenoth.

T. HELLESETH

On some ternary m-sequences with good autocorrelation and crosscorrelation

Let $\{s_t\}$ be an m-sequence of period 3^n-1 with elements $0,1,2$ and let $\{s_{dt}\}$ denote another ternary m-sequence of period 3^n-1, i.e., $(d, 3^n-1)=1$. The crosscorrelation is given by

$$C_d(\tau) \;=\; \sum_{t=0}^{3^n-2} \omega^{s_{t+\tau}-s_{dt}}, \quad \omega = \exp(\frac{2\pi i}{3})$$

(if $d=3^j$, then both sequences are the same and we will call it an autocorrelation).

Theorem 1 Let $d = 2\cdot 3^m+1$ where $n=2m+1$, then the crosscorrelation function $C_d(\tau)$ takes on the following three values:

$$\begin{array}{ccc} 1+3^{m+1} & \text{occurs} & \frac{1}{2}(3^{n-1}+3^m) \text{ times} \\ -1 & \text{occurs} & 3^n-3^{n-1}-1 \text{ times} \\ -1-3^{m+1} & \text{occurs} & \frac{1}{2}(3^{n-1}-3^m) \text{ times}. \end{array}$$

Theorem 2 Let $d=3^{2k}-3^k+1$, $n=3k$, then the ternary sequence

$$u_t \;=\; s_t + s_{dt}$$

has ideal two-level autocorrelation (being -1 for all shifts $\neq 0$).

T. HØHOLDT

List decoding of Reed-Solomon codes

We survey the recent work on the implementation of M. Sudan's (1997) algorithm for list decoding of Reed-Solomon codes and report on recent results by J. Justesen and the author on bounds of list decoding of MDS-codes. The main results are that Sudan's bound is tight in the sense that for a given rate r there exists Reed-Solomon codes of that rate such that the maximal fractional number of errors that can be corrected with bounded lists is at most $1 - \sqrt{r}$.. For lists of size j we prove the corresponding results. We also show that with random codes (over large fields) one can do better.

R. KÖTTER and A. VARDY

Algebraic soft-decision decoding of Reed-Solomon Codes

We define a polynomial-time soft-decision decoding algorithm for Reed-Solomon codes. The algorithm is algebraic in nature and builds upon the interpolation procedure proposed by Guruswami and Sudan for hard-decision decoding. Algebraic soft-decision information is achieved by means of converting the soft-decision reliability information into a set of interpolation points along with their multiplicities. The proposed conversion procedure is shown to be optimal for a certain probabilistic model. Asymptotic analysis for a large number of interpolation points is presented culminating in a complete characterization of the decoding regions of the proposed algorithm. The algorithm easily extends to polynomial-time soft-decision decoding of BCH codes and codes from algebraic curves.

H.-A. LOELIGER

Turbo codes and related topics

The invention of "turbo codes" by Berrou et al. (1993) has moved the practically achievable data rates much closer to the information-theoretic channel capacity than was previously believed possible. Shortly after the invention of turbo codes, it was discovered experimentally by MacKay that Gallager's "low-density parity check (ldp) codes" from 1963 were almost as good as turbo codes. In fact, recent refinements (irregular ldp codes) have improved ldp codes well beyond turbo codes. The old vision, put forth by Shannon, of nearly capacity achieving codes has thus finally turned into a practical reality. A pivotal element of these developments is the generic "sum-product" or "probability propagation" decoding algorithm, which operates by "message passing" on a graphical model (the "Tanner graph" or "factor graph") of the code. This algorithm and such graphical models are applicable also beyond coding.

H.-G. RÜCK

On the discrete logarithm in Jacobians

For various cryptographic protocols one needs a cyclic group G of prime order m, in which the "exponentation" $n \mapsto n \cdot P$ is a one-way function. The inverse, in multiplicative terms the "discrete logarithm" should be hard to compute. We discussed various presentations of the cyclic group G, such as the additive group ($G = \mathbb{Z}/m\mathbb{Z}$), the multiplicative group ($G \subset \mathbb{F}_q^*$) and the Jacobians ($G \subset J(\mathbb{F}_q)$) of algebraic curves over a finite field $\mathbb{F}_q$. In general the discrete logarithm in Jacobians is thought to be more secure than in the other groups. We showed that nevertheless one has to be careful when choosing the curve and its Jacobian. In particular one should avoid the cases $m|q-1$ and $m|q$.

A. SHOKROLLAHI

Iterative decoding of LDPC codes

In the last few years low-density parity-check codes have occupied centerstage in the coding theory community. This has been mostly due to simple and efficient encoding and decoding algorithms which allow constructing codes which allow transmitting at rates extremely close to Shannon capacity. In this talk, I will review the constructions and elaborate on some of the proof techniques regarding the decoding algorithms.

P. SOLÉ

Self-dual codes over rings: recent results

These codes yield modular lattices via Construction A and codes over fields by Gray map. Four topics were treated:

1. 2-modular lattices from codes over $F_3 \times F_3$
2. Type II binary codes from Euclidean self-dual codes over F_4
3. Type IV codes over the three nonfield rings of order 4
4. Duadic codes over Z_4

S. A. STEPANOV

Modular invariants of finite groups

Let R be a commutative ring with identity, $A_{mn} = R[x_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq n]$, and $G \leq GL(R, n)$ a finite group acting on the polynomial R-algebra A_{mn} via linear transformations of variables $x_{i1}, \ldots, x_{in}$ (which are the same for any $i = 1, 2, \ldots, m$). If R is Noetherian, it follows from the Hilbert-Noether finiteness theorem that the ring A_{mn}^G of invariants of G is a finitely generated commutative R-algebra and A_{mn} is finitely generated as a module over A_{mn}^G. Moreover, if $|G|$ is invertible in R then A_{mn}^G is generated over R by polynomials of degree $\leq |G|$, no matter how large m is (P. Fleischmann, 2000). In *modular case* when $|G|$ is not invertible in R there is no degree bound for generators of A_{mn}^G that is independent of m. More precisely, if R is a field of prime characteristic p and p divides $|G|$ then every system of R-algebra generators of A_{mn}^G contains a generator whose degree $\geq cm$ for some $c = c(p, |G|) > 0$ (D. Richman, 1996). The purpose of this talk is to devote some new arithmetical ideas which allow to simplify Richman's arguments and to sharpen his lower bound. The results give a possibility to construct smooth projective curves over finite fields with many rational points.

M. SUDAN

List decoding of error-correcting codes

Given an error-correcting code C, a received vector $\underline{r}$, and an error bound e, the list decoding problem is that of recovering all codewords of C within a Hamming distance of e from $\underline{r}$. This problem generalizes the classical problem of unambigious decoding and offers an avenue to "decode" more errors than half the minimum distance of the code C. In this talk we describe list-decoding algorithms for a wide class of algebraic codes that decode when the number of errors is significantly larger than half the minimum distance. Parts of this talk are joint with Venkatesan Guruswami and Amit Sahni.

R. URBANKE

Iterative coding systems

In this talk we will survey what is known about iterative coding systems. In particular we will concentrate on the class of turbo codes and repeat accumulate codes. We will see that the asymptotic case (large lengths n) is fairly well understood but that very little is known for small block lengths. In the asymptotic setting the main tools of analysis are a concentration theorem as well as the density evolution process to determine the threshold of iterative coding systems. This talk is based on joint work with various people (Tom Richardson, Amin Shokrollahi, Sae-Young Chung, Louay Bazzi, Cyrill Measson).

W. WILLEMS

Codes with a large gap in the weight distribution

Given two codes C and C' with parameters $[n,k,d]_q$ and $[n,k,d']_q$. Which code should we use in order to minimize the probability of an incorrect decoding if we decode up to $t \leq \min(\frac{d-1}{2}, \frac{d'-1}{2})$ errors? This question has recently been answered by Faldum, namely C has smaller decoding error probability than C' if and only if $(A_0, \ldots, A_n) < (A'_0, \ldots, A'_n)$ in lexicographical order where A_i, A'_i denotes the weight distribution of the corresponding code. So-called MMD codes - codes which have a large gap in the weight distribution, i.e $A_{d+1} = \ldots = A_{n-d^\perp+1} = 0$ - have smallest decoding error probability in the class of $[n,k,d]$ codes. A complete list of all MMD codes is given. Furthermore almost MMD codes are discussed in connection with the existence of Steiner systems.

C. XING

Sequences from curves over finite fields

Curves over finite fields have found many interesting applications in various areas. In the talk, constructions of d-perfect sequences are given based on curves over finite fields.

M. ZIEVE

Curves of every genus with many points

In the 1940's, Weil showed that a curve over F_q of genus g has at most $q+1+2g\sqrt{q}$ rational points. This bound was dramatically improved (for small q) around 1980, by means of coding theory: Goppa used curves with many points to construct codes with good parameters, and improvements to the Weil bound result from translating known bounds on parameters of codes. This inspired the converse question of producing curves with many points, to test how much further the Weil bound could be improved. Our main result is that, for fixed q, the Weil bound can only be improved by a constant factor: **Theorem** For every q and g, there is a curve over F_q of genus g having at least $c_q \cdot g$ rational points, where c_q is a positive constant depending only on q. This resolves a 1983 question of Serre. Previously Ihara (for square q) and Serre (for all q) had shown that, for fixed q, the conclusion of our result at least held for an infinite set of genera g.

This is joint work with N. Elkies, A. Kresch, B. Poonen, and J. Wetherell.

Berichterstatter: G. van der Geer, P. V. Kumar

E-Mail Addresses

Aleshnikov, Ilia	mat314@uni-essen.de
Auer, Roland	auer@math.rug.nl
Barbero, Angela	angbar@wmatem.eis.uva.es
Barg, Alexander	alexanderbarg@lucent.com
Beelen, Peter	p.h.t.beelen@tue.nl
Bierbrauer, Jürgen	jbierbra@mtu.edu
Charpin, Pascale	pascale.charpin@inria.fr
Dillon, John F.	jfdillon@afterlife.ncsc.mil
Duursma, Iwan	duursma@unilim.fr
Farran, J. Ignacio	ignfar@eis.uva.es
Forney, David	forneyd@mediaone.net
Garcia, Arnaldo	garcia@impa.br
Gong, Guang	ggong@cacr.math.uwaterloo.ca
Helleseth, Tor	torh@ii.uib.no
Høholdt, Tom	T.Hoeholdt@mat.dtu.dk
Hübl, Reinhold	reinhold.huebl@mathematik.uni-regensburg.de
Kötter, Ralf	koetter@uiuc.edu
Kumar, P. Vijay	vijayk@usc.edu
Ling, San	lings@math.nus.edu.sg
Loeliger, Hans-Andrea	loeliger@isi.ee.ethz.ch
Mattig, Lena	lenamattig@uni-essen.de
Moreno, Oscar	o_moreno@upr1.upr.clu.edu
Munuera, Carlos	cmunuera@modular.arg.uva.es
Özbudak, Ferruh	ozbudak@math.metu.edu.tr
Paoluzi, Maurizio	paoluzi@mat.uniroma2.it
Pott, Alexander	alexander.pott@mathematik.uni-magdeburg.de
Rueck, Hans-Georg	rueck@exp-math.uni-essen.de
Schoof, René	schoof@wins.uva.nl
Shabat, Vasily	shabat@wins.uva.nl
Shokrollahi, Amin	amin@research.bell-labs.com
Solé, Patrick	ps@essi.fr
Sudan, Madhu	madhu@mit.edu
Stepanov, Serguei	stepanov@fen.bilkent.edu.tr
Stichtenoth, Henning	stichtenoth@uni-essen.de
Urbanke, Rüdiger	Rudiger.Urbanke@epfl.ch
van der Geer, Gerard	geer@science.uva.nl
Vardy, Alexander	vardy@ece.ucsd.edu
Walker, Judy	jwalker@math.unl.edu
Willems, Wolfgang	wolfgang.willems@mathematik.uni-magdeburg.de
Wolfmann, Jacques	wolfmann@univ-tln.fr
Xing, Chaoping	matxcp@nus.edu.sg
Ytrehus, Øyvind	oyvind@ii.uib.no
Zieve, Michael	zieve@idaccr.org

Participants

Prof. Dr. Ilia Aleshnikov
FB 6 - Mathematik und Informatik
Universität-GH Essen
45117 Essen

Prof. Dr. Roland Auer
Afdeling voor Wiskunde
Rijksuniversiteit Groningen
Postbus 800
NL-9700 AV Groningen

Prof. Dr. Angela Barbero
Dept. Matematica Aplicada
Ingeniero Indust.
Paseo del Cauce s/n
E-47011 Valladolid

Prof. Dr. Alexander Barg
Bell Labs, Lucent Technologies
Room 2C-375
600 Mountain Avenue
Murray Hill , Nj 07974
USA

Peter Beelen
Vakgroep Discrete Wiskunde
TU Eindhoven
Postbus 513
NL-5600 MB Eindhoven

Dr. Jürgen Bierbrauer
Institut für Mathematik
Universität Salzburg
Hellbrunnerstr. 34
A-5020 Salzburg

Prof. Dr. Pascale Charpin
Projet CODES
Institut National de Recherche
en Informatique Autonomique
INRIA
F-78153 Le Chesnay Rocquencourt

Dr. John F. Dillon
National Security Agency
Office of Mathematical Research
R51
Fort George G. Meade MD 20755
USA

Prof. Dr. Hans Dobbertin
Masurenweg 5
53119 Bonn

Dr. Iwan Duursma
Mathematics Department
University of Limoges
123, avenue Albert Thomas
F-87060 Limoges

Dr. J. Ignacio Farran
c/o Prof. Dr. G.M. Greuel
FB Mathematik
Universität Kaiserslautern
67653 Kaiserslautern

Dr. David Forney
1010 Memorial Drive
Apt. 3G
Cambridge , MA 02138
USA

Prof. Dr. Arnaldo Garcia
Institute of Pure and Applied Math.
IMPA
Estrada Dona Castorina 110
Rio de Janeiro RJ 22460-320
BRAZIL

Prof. Dr. Gerard van der Geer
Fakulteit Wiskunde en Informatica
Universiteit van Amsterdam
Plantage Muidergracht 24
NL-1018 TV Amsterdam

Prof. Dr. Guang Gong
Department of Combinatorics and
Optimization
University of Waterloo
Waterloo , Ont. N2L 3G1
CANADA

Prof. Dr. Tor Helleseth
Department of Informatics
University of Bergen
Hoyteknologisenteret
N-5020 Bergen

Prof. Dr. Tom Hoeholdt
Department of Mathematics
Technical University of Denmark
Bldg. 303
DK-2800 Lyngby

Dr. Reinhold Hübl
Fakultät für Mathematik
Universität Regensburg
Universitätsstr. 31
93053 Regensburg

Prof. Dr. Ralf Kötter
Coordinated Science Laboratory
University of Illinois at
Urbana-Champaign
1101 W. Springfield Avenue
Urbana , IL 61801
USA

Prof. Dr. Vijay Kumar
Communication Sciences Institute
University of Southern California
Electr. Engineering Dept. -Systems
University Park
Los Angeles , CA 90089
USA

Prof. Dr. San Ling
CNRS-I3S
ESSI
B.P. 145
Route des Colles
F-06903 Sophia Antipolis Cedex

Prof. Dr. Hans-Andrea Loeliger
Eidmattstrasse 51
CH-8032 Zürich

Lena Mattig
FB 6 - Mathematik und Informatik
Universität-GH Essen
45117 Essen

Prof. Dr. Oscar Moreno
Dept. of Mathematics
Faculty of Natural Sciences
University of Puerto Rico
Box 23355
Rio Piedras , PR 00931
USA

Prof. Dr. Carlos Munuera
Dept. Matematica Aplicada
E.T.S. Arquitectura
Avda. Salamanca s/n
E-47014 Valladolid

Prof. Dr. Ferruh Özbudak
Dept. of Mathematics
Middle East Technical University
06531 Ankara
TURKEY

Dr. Maurizio Paoluzi
Dipartimento di Matematica
Universita degli Studi di Roma
Tor Vergata
Via della Ricerca Scientifica
I-00133 Roma

Prof. Dr. Alexander Pott
Fakultät für Mathematik
Otto-von-Guericke-Universität
Magdeburg
Postfach 4120
39016 Magdeburg

Dr. Hans-Georg Rück
Institut für Experimentelle
Mathematik
Universität-Gesamthochschule Essen
Ellernstr. 29
45326 Essen

Prof. Dr. Rene Schoof
Dipartimento di Matematica
2. Universita di Roma
"TOR VERGATA"
I-00185 Roma

Dr. Vasily Shabat
Korteweg-de-Vries Instituut
Universiteit van Amsterdam
Plantage Muidergracht 24
NL-1018 TV Amsterdam

Dr. Amin Shokrollahi
Bell Labs, 2C-381
Lucent Technologies
700 Mountain Ave
Murray Hill , NJ 07974
USA

Prof. Dr. Patrick Sole
Laboratoire d'Informatique
Signaux et Systems de
Sophia Antipolis (I3S)
250, rue Albert Einstein
F-06560 Valbonne

Prof. Dr. Sergei A. Stepanov
Department of Mathematics
Bilkent University
06533 Ankara
TURKEY

Prof. Dr. Henning Stichtenoth
FB 6 - Mathematik und Informatik
Universität-GH Essen
45117 Essen

Prof. Dr. Madhu Sudan
Lab. for Computer Science
MIT
NE43-332
545 Tech Square
Cambridge , MA 02139
USA

Dr. Rudy Urbanke
Communications Theory Laboratory
LTHC - DSC - INR
CH-1015 Lausanne

Prof. Dr. Alexander Vardy
Dept. of Electrical Engineering
University of California, San Diego
9500 Gilman Drive, MC 0407
La Jolla , CA 92093-0112
USA

Prof. Dr. Judy Walker
Department of Mathematics and
Statistics
University of Nebraska, Lincoln
Lincoln , NE 68588
USA

Prof. Dr. Wolfgang Willems
Fakultät für Mathematik
Otto-von-Guericke-Universität
Magdeburg
Universitätsplatz 2
39106 Magdeburg

Prof. Dr. Jacques Wolfmann
GECT
Universite de Toulon et du Var
Chateau St. Michel
F-83130 La Garde

Prof. Dr. Chaoping Xing
Department of Mathematics
National University of Singapore
Science Drive 2
Singapore 117543
SINGAPORE

Prof. Dr. Oyvind Ytrehus
Department of Informatics
University of Bergen
Hoyteknologisenteret
N-5020 Bergen

Dr. Michael Zieve
Center for Communications Research
29 Thanet Rd.
Princeton , NJ 08550
USA