

TP14-53
I43,2
1997

9860436

**Proceedings
1997 IEEE
International Symposium on
Information Theory**

图书馆藏书

**Maritim Hotel and Congress Center
Ulm, Germany**

June 29 - July 4, 1997

Sponsored by The Information Theory Society of
The Institute of Electrical and Electronics Engineers



E9860436

Proceedings 1997 IEEE International Symposium on Information Theory

Copyright and Reprint Permission: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923. For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331. All rights reserved. Copyright ©1997 by the Institute of Electrical and Electronics Engineers, Inc.

IEEE Catalog Number: 97CH36074

ISBN:	0-7803-3956-8	Softbound Edition
	0-7803-3957-6	Casebound Edition
	0-7803-3958-4	Microfiche Edition

Library of Congress: 72-179437

Additional copies of this publication are available from

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08854-1331
1-800-678-IEEE

Chairmen

Daniel Costello, Bernhard Dorsch, Han Vinck

Finance:

Martin Bossert

Registration:

Martin Bossert, Han Vinck

Publications and Publicity:

Werner Henkel, Klaus Huber

Local Arrangements:

Jürgen Lindner

International Advisory Committee:

Rolf Johannesson

Acknowledgements

Grateful acknowledgement is given to the following organizations for their financial support of the 1997 IEEE ISIT:

AEG Mobile Communication, Ulm

Alcatel SEL, Stuttgart

City of Ulm

Daimler Benz Research Institute, Ulm

Daimler Benz Aerospace, Ulm

Deutsche Telekom AG, Ulm

E Plus Mobilfunk GmbH, Düsseldorf

Mannesmann Mobilfunk GmbH, Stuttgart

NASA Ames Research Center, Maffett Field, CA, USA

Siemens AG, Munich

Siemens AG, Ulm

The National Science Foundation, USA

Ulmer Universitätsgesellschaft

University of Ulm

Program Committee

Joachim Hagenauer (Chairman)
Henk van Tilborg (Chairman)
Rudolph Ahlswede
John Anderson
Ezio Biglieri
Martin Bossert
Pierre Chevillat
Daniel Costello
Ilya Dumer
Tony Ephremides
David Forney
Costas Georghiades
Christoph Günther
Te Sun Han
Kees Schouhamer Immink
Rolf Johannesson
Ralf Kötter
Torleiv Kløve
Shu Lin
Jim Massey
Ueli Maurer
Edward van der Meulen
Heinrich Meyr
Jim Modestino
Ben Smeets
Aimo Tietäväinen
Gottfried Ungerböck
Frans Willems
Ephraim Zehavi

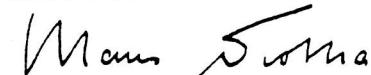
Schriftliches Grußwort von Herrn Minister

Klaus von Trotha

für den Tagungsband „ISIT ‘97“ in Ulm

It is my pleasure to welcome the IEEE Information Theory Society to Baden-Württemberg for its International Symposium on Information Theory. It shows that the German scientists working in this field have major contributions to this growing area of science. The presence of so many well known researchers in the field will definitely stimulate our students to start or continue their studies in this direction of Information Sciences on a high level. The IEEE German Chapter on Information Theory has about 200 members, highlighting the importance of the Information Theory Society for the local scientific community. Germany has a great tradition in research, and Information theory plays an important role in the fields of Mathematics and Communications. Several publications by Claude Shannon have appeared in German technical journals. A well-known meeting point for Information theorists is the Oberwolfach conference center in the beautiful Black Forest, not far from Stuttgart. I am sure that many new contacts will be made at this Symposium, not only between scientists, but also between science and industry. The choice of the city of Ulm as venue is an excellent one from several points of view.

Ulm is a city dedicated to science with many research establishments and a young university. It has been chosen to be the city where research in multimedia applications will be concentrated in the near future. Ulm is in the middle of a number of very exciting attractions. I hope that you will take the opportunity to visit a few of these and that your stay will be a profitable one, both from a scientific as well as from a cultural point of view. I conclude using the famous Ulmer saying that it is „In Ulm, um Ulm, und um Ulm herum“, where the action is!



Klaus von Trotha

Minister für Wissenschaft, Forschung und Kunst
des Landes Baden-Württemberg

Table of Contents

Plenary Session I

- The Way to the Proof of Fermat's Theorem — Frey, G. 1

Shannon Lecture I

- Information Theoretic Methods in Probability and Statistics — Csiszár, I. 2

Plenary Session II

- Practical Implementations of Cryptography — Landrock, P. 3

Shannon Lecture II

- Back from Infinity: A Constrained Resources Approach to Information Theory — Ziv, J. 4

Plenary Session III

- Source Coding in Multimedia — Rabiner, L.R. 5

Session MOAM1 Iterative Decoding

- A General Algorithm for Distributing Information in a Graph — Aji, S.M. and McEliece, R.J. 6

Soft-Input Soft-Output Building Blocks to Construct and Iteratively Decode Code Networks —

- Benedetto, S. and Montorsi, G. 7

Serial Concatenated Trellis Coded Modulation with Iterative Decoding —

- Benedetto, S., Divsalar, D., Montorsi, G., and Pollara, F. 8

On the Performance of Recursive Decoding Schemes — Soljanin, E. and Urbanke, R. 9

Hybrid Concatenated Codes and Iterative Decoding — Divsalar, D. and Pollara, F. 10

Simultaneous Decoding and Phase Synchronization Using Iterative "Turbo" Decoding — Wiberg, N. 11

Approaching Shannon's Capacity Limit by 0.27 dB Using Hamming Codes in a 'Turbo'-Decoding Scheme — Nickl, H., Hagenauer, J., and Burkert, F. 12

Session MOAM2 Combinatorics and Sequences

- Modularity Properties of Graph Entropy — Körner, J. and Simonyi, G. 13

Correlation Attacks on Stream Ciphers Using the Lempel-Ziv Algorithm — Penzhorn, W.T. 14

Pseudoredundant Measurements in Nonlinear Mappings — Arndt, C. and Loffeld, O. 15

On Higher Order Autocorrelation Properties of Golay Complementary Sequences — Braun, V. 16

Design of Sequences of I.I.D. p -ary Random Variables — Kohda, T. and Tsuneda, A. 17

Multiple Packing of Euclidean Sphere — Blinovsky, V. 18

Enumeration of Rare Events, Pyramid and Ball Cubic Lattices — Krichevskii, R.E. and Potapov, V.N. 19

On Efficient Inversion in Tower Fields of Characteristic Two — Fan, J.L. and Paar, C. 20

Data-Punctuated Token Trees — Berlekamp, E. and Hekuis, P. 21

Session MOAM3 Multi-User Channels

Arbitrarily Varying Multiple-Access Channels Part I. Ericson's Symmetrizability is Adequate, Gubner's Conjecture is True. — Ahlswede, R. and Cai, N. 22

Arbitrarily Varying Multiple-Access Channels Part II. Correlated Sender's Side Information, Correlated Messages, and Ambiguous Transmission — Ahlswede, R. and Cai, N. 23

Approximating the Output of the Multiple Access Channel — Steinberg, Y. 24

A New Perspective to AWGN Multi-Access Channels — Shu, L. 25

Generalized Time Sharing for Multiple Access Channels — Rimoldi, B. 26

Optimal Power Allocation over Parallel Gaussian Broadcast Channels — Tse, D.N. 27

The Capacity Region of Broadcast Channels with Memory — Goldsmith, A. and Effros, M.	28
A 2-D Weighing Procedure for Two-Way Communication — Schalkwijk, J.P.M. and Meeuwissen, H.B.	29
Iterative Multi-User Decoding for Asynchronous Users — Tarköy, F.	30

Session MOAM4 Communication Networks

Buffer Occupancy of Statistical Multiplexers with Periodic Interchangeable Traffic in ATM Networks — Yu, Z. and McEliece, R.J.	31
Transmission of Messages Using Parallel Servers: Asymptotic Approach — Vvedenskaya, N.D.	32
Large Deviations Analysis of MMPP/D/1 Queueing — Nakagawa, K.	33
An Independent Window-Access Scheme for an Input-Buffered Fast Packet Switching Fabric — Liu, Y.-S., Liu, Z.-J., and Hu, Z.	34
A New Toroidal Multi-Dimensional Network — Lee, L.L. and Centeno Filho, A.J.	35
A Distributed Optimal Routing Strategy Based on Estimation of the OD Matrix — Adibniya F.	36
Events with Exponentially Vanishing Probability have Exponentially Growing Waiting Time — Algoet, P.	37
Information Aging — Daneshgaran, F. and Mondin, M.	38

Session MOAM5 Sequences

Greedy Algorithms for the Shortest Common Superstring That are Asymptotically Optimal — Frieze, A. and Szpankowski, W.	39
Large Linear Complexity Sequences over Z_8 — Martinsen, H.M.	40
Periodic Binary Sequences with the "Trinomial Property" — Golomb, S.W. and Gong, G.	41
On the Classification of Binary Sequences of Period $2^n - 1$ with Ideal Autocorrelation — No, J.-S., Lee, H.-K., Chung, H., Yang, K., and Song, H.-Y.	42
On Cyclic Goppa Codes and Sequence Designs — Moreno, O.	43
Correlations of Pseudo-Generalized Geometric Sequences — Sun, W. and Yang, Y.X.	44
The Distribution of the Degree of Minimum-Degree Low-Weight Parity-Check Polynomials — Kühn, G.J.	45

Session MOAM6 CDMA I

Carrier Suppressed RAKE Receiver Operation for CDMA Cellular Communications — Kong, N.	46
Maximum Number of Users of a Random Signatures CDMA System with Adaptive Array Receivers over Multipath Fading Channel — Rapajic, P. and Kennedy R.	47
On Coherent Reception of Up-link Transmitted Signals in the DS-CDMA System — Jimenez, A. and Zigangirov, K.Sh.	48
A Multistage Detector for Synchronous Code-Division Multiple-Access — Louichon, F. and Georghiades, C.N.	49
Whitening Sequences in DS Spread Spectrum Communication — Hovakimyan, K.S. and Khachatrian, G.H.	50
MMSE Reception of DS-CDMA for Frequency-Selective Fading Channels — Miller, S.L., Honig, M.L., Shensa, M.J., and Milstein, L.B.	51
Complexity-Constrained Maximum-Likelihood Detection in Multiuser CDMA — Rasmussen, L.K., Lim, T.J., and Aulin, T.M.	52
(L,K) CDMA/ALOHA Multiple-Access System — Alrumaih, R.M. and Alsugair, A.A.	53

Shannon-Based Capacity Estimations of Future Microcellular Wireless Communication Systems — Hammerschmidt, J.S., Hasholzner, R., and Drewes, C.	54
Session MOAM7 Quantization I	
Asymptotic Performance of Vector Quantizers with the Perceptual Distortion Measure — Li, J., Chaddha, N. and Gray, R.M.	55
Lattice Labeling Algorithms for Vector Quantization — Wang, C., Cao, H.Q., Li, W., and Tzeng, K.K.	56
Context-Based Entropy Coding of VQ Indexes — Wu, X., Wen, J., and NG, W.	57
Entropy Coded Successively Refinable Uniform Threshold Quantizers — Brunk, H., Jafarkhani, H., and Farvardin, N.	58
Quantization of Both Stationary and Nonstationary Gaussian Sources with Voronoi Constellations — Pépin, C., Belfiore, J.-C., and Boutros, J.	59
Polar Quantization Revisited — Neuhoff, D.L.	60
Low-Complexity Waveform Coding via Alphabet and Sample-Set Partitioning — Said, A. and Pearlman, W.A.	61
Structured Spherical Codes for Gaussian Quantization — Hamkins, J. and Zeger, K.	62
Session MOAM8 Compaction Methods	
The Imaginary Sliding Window — Ryabko, B.	63
Context-Tree Weighting for Text-Sources — Wolf, P.A.J.	64
Estimation of Escape Probabilities for PPM Based on Universal Source Coding Theory — Åberg, J., Shtarkov, Yu, M., and Smeets, B.J.M.	65
Ordering the Probabilities of an Unknown Discrete Memoryless Source — Sayir, J. and Ernst, T.	66
Two Results in Text Compression Algorithms — Wong, L., Wei, V.K., and Yeung, R.W.	67
Live-and-Die Coding for Binary Piecewise I.I.D. Sources — Willems, F. and Krom, M.	68
Lossless Volume Compression Using a Variation of Lempel-Ziv '77 — Chow, J. and Berger, T.	69
Universal Probability Assignment in the Class of Two-Sided Geometric Distributions — Merhav, N., Seroussi, G., and Weinberger, M.J.	70
Optimal Prefix Codes for Two-Sided Geometric Distributions — Merhav, N., Seroussi, G., and Weinberger, M.J.	71
Session MOPM1 Signal Theory	
Error-Free Filtering of Entropy-Regular Process against a Background of Entropy-Singular Noise — Pinsker, M.S. and Prelov, V.V.	72
Sensitivity of the Rate-Distortion Function of Stationary Continuous-Time Gaussian Processes to Non-Gaussian Contamination — Pinsker, M.S., Prelov, V.V., and Verdú, S.	73
Robust Estimation of Point Process Intensity Features Using k -minimal Spanning Trees — Hero, A.O. and Michel, O.	74
Making MLSD-Decisions on Some Individual Symbols in a Sequence by Thresholding the Matched Filter Output — Ödling, P., Eriksson, H.B., and Börjesson, P.O.	75
Limitations of the Gaussian Model for Radar Signals — Nayebi, M.M. and Aref, M.R.	76
Nonlinear ECG Filtering by Group Normalized Wavelet Packets — Zhuoer, S., Zheng, B., Licheng, J., and Kun, M.	77
Estimation of Sampling Jitter Variance using Autocorrelation Function and Higher Order Statistics — Guerrero, A.P., Tourneret, J.-Y., and Aakvaag, N.	78

New Results on the Expected Number of Maxima in the Normal Process Envelope — Nader-Esfahani, S. and Abdi, A.	79
On Algebraic Properties of Selfreciprocal Polynomials and of Daubechies Filters of Low Order — Klappenecker, A.	80
Session MOPM2 Bounds on Codes	
Linear Programming Bounds for Codes in Infinite Projective Spaces — Boyvalenkov, P., Danev, D., and Mitradjieva, M.	81
An Improved Serre Bound for Elementary Abelian Extensions of $F_q(x)$ and the Generalized Hamming Weights of Duals of BCH Codes — Moreno, O., Pedersen, J.P., and Polemi, D.	82
Information-Theoretic Bounds on Trellis Complexity of Nonlinear Codes — Reuven, I. and Be'ery, Y.	83
On Upper Bounds for the Distance of Codes of Small Size — Krasikov, I. and Litsyn, S.	84
Improved Bounds for Ternary Linear Codes of Dimension 7 — Gulliver, T.A. and Östergård, P.R.J.	85
On the Minimal Words of the Primitive BCH Codes — Borissov, Y. and Manev, N.L.	86
Some New Bounds for Q -ary $[n, k, d]$ Codes — Ma, X. and Wang, X.	87
Session MOPM3 Cryptology I	
The Intrinsic Conditional Mutual Information and Perfect Secrecy — Maurer, U. and Wolf, S.	88
The Optimal Linear Worst-Case Information Rate — van Dijk, M.	89
MDS Secret Sharing Schemes Secure against Cheaters — Okada, K. and Kurosawa, K.	90
Smoothing Probability Distributions and Smooth Entropy — Cachin, C. and Maurer, U.	91
High Rate Reconciliation — van Dijk, M. and Koppelaar, A.	92
On the Entropy Bound for Optimum Homophonic Substitution — da Rocha Jr., V.C. and Massey, J.L.	93
Decreasing Redundancy of Homophonic Coding — Ryabko, B. and Fionov, A.	94
New Authenticated Key Distribution Scheme and Secure Broadcast Scheme — Xu, S.-b. and Wang, X.-m.	95
Session MOPM4 Coded Modulation I	
Bit-Interleaved Coded Modulation — Caire, G., Taricco, G., and Biglieri, E.	96
Bandwidth-Efficient Trellis-Coded Modulation Schemes with Prescribed Decoding Delay — Li, Q. and Rimoldi, B.	97
Trellis Matched Codes for Partial Response Channels — Uchôa Filho, B.F. and Herro, M.A.	98
Code Partial Response CPFSK with Ring Convolutional Codes — Remlein, P.	99
Analysis and Design of Trellis Codes Optimized for a Binary Symmetric Markov Source with MAP Detection — Kroll, J.M. and Phamdo, N.	100
Unequal Error Protection Scheme Using Several Convolutional Codes — Matsunaga, M., Asano, D.K., and Kohno, R.	101
Performance of Coded Modulation Schemes Using Multiple Transmit Antennas — Ramésh, R.	102
Multilevel Coding for Peak Power Limited Complex Gaussian Channels — Müller, R.R., Wachsmann, U., and Huber, J.B.	103
Session MOPM5 Parallel and Serial Concatenation	
On Optimal Power Allocation for Turbo Codes — Duman, T.M. and Salehi, M.	104
On the Ensemble Performance of Turbo Codes — Telatar, E. and Urbanke, R.	105
Serial Concatenation of Interleaved Codes: Performance Analysis, Design and Iterative Decoding — Benedetto, S., Divsalar, D., Montorsi, G., and Pollara, F.	106

Active Distances and Cascaded Convolutional Codes — Höst, S., Johannesson, R., Zigangirov, K.Sh., and Zyablov, V.V.	107
On the Distribution of the Output Error Burst Lengths for Viterbi Decoding of Convolutional Codes — Höst, S., Johannesson, R., Zigangirov, D.K., Zigangirov, K.Sh., and Zyablov, V.V.	108
New Turbo-Like Codes — Loeliger, H.-A.	109
Serial Concatenation of Convolutional Code and Low Rate Orthogonal Convolutional Code — Li, J. and Imai, H.	110
Graph Theoretic Construction of Generalized Product Codes — Guinand, P.S. and Lodge, J.H.	111
Multilevel Turbo Coding with a Short Latency — Herzberg, H.	112
Session MOPM6 Code Constructions	
Good Error-Correcting Codes Based on Very Sparse Matrices — MacKay, D.J.C.	113
Some Geometric Constructions of Optimal Quaternary Codes — Hill, R. and Lizak, P.	114
Error Correction for Semiconductor Memories — Tolhuizen, L. and Baggen, S.	115
Some New Extremal Self-Dual Codes with Length 58 — Buyuklieva, S.	116
Spectral Techniques for Expander Codes and Generalized Cyclic Codes — Lafferty, J.D. and Rockmore, D.N.	117
Superimposed Codes are Almost Big Distance Ones — Füredi, Z. and Ruszinkó, M.	118
Three New Binary Linear Codes — Boukliov, I.	119
Session MOPM7 Frequency Hopping and Multicarrier Systems	
Forward Error Correction with Reduction of Peak to Average Power Ratio of QPSK Multicarrier Signals — Ochiai, H. and Imai, H.	120
Time-Limited Waveforms for OFDM-CDMA in a Multipath Fading Channel — Drakul, S.L.	121
Algorithms for Carrier Acquisition for QAM Constellations — Preston, J. and Georghiades, C.N.	122
Two-Dimensional Pilot-Symbol-Aided Channel Estimation — Hoher, P., Kaiser, S., and Robertson, P.	123
Soft Handoff Technique for Mobile Multi-Carrier CDMA Systems — Atarashi, H. and Nakagawa, M.	124
A Class of Frequency-Hop Patterns — Sarwate, D.V. and Losada, D.A.	125
A Class of Frequency Hop Codes with Nearly Ideal Characteristics for Multiple-Target Recognition — Moreno, O. and Marić, S.	126
A Class of Frequency Hop Codes Using Only Three Frequencies — Moreno, O., Marić, S., and Corrada, C.J.	127
Mismatched Frequency Hopping Sequences for Radars and Sonars — Zejak, A.J., Simić, I.S., and Dukić, M.L.	128
Session MOPM8 Channels with Feedback	
Coding for Channels with Low Rate Noiseless Feedback — Bargh, M.S. and Schalkwijk, J.P.M.	129
On the Cover's Conjecture of Gaussian Feedback Capacity — Yanagi, K.	130
A Sequential Strategy for the Two-User Noiseless Binary Adder Channel with Feedback — Kramer, G.	131
The AVC with Noiseless Feedback and Maximal Error Probability: A Capacity Formula with a Trichotomy — Ahlswede, R. and Cai, N.	132
Fast Iterative Coding for Feedback Channels — Ooi, J.M. and Wornell, G.W.	133
Reliability and Throughput Analysis of ARQ Schemes in Burst Error Channels — Zepernick, H.-J.	134
The Value of Adaptive Questions in Generalized Mastermind — Roche, J.R.	135
Experimental Study of Ants Numerical Aptitude Based on the Ideas of the Information Theory —	

Ryabko, B. and Reznikova, Z.	136
Session TUAM1 Recording & Line Codes I	
Reduced Complexity MLSD Algorithms for Multi-Track Magnetic Recording Systems — Kurtas, E., Proakis, J.G., and Salehi, M.	137
Multi-Track Codes for Magnetic Recording Systems with Servo Positioning Errors — Kurtas, E., Proakis, J.G., and Salehi, M.	138
Channel Capacity of M -ary Multitrack Runlength Limited Channels — Vasic, B.V., McLaughlin, S.W., and Milenovic, O.	139
Lower Bounds on the Anticipation of Encoders for Input-Constrained Channels — Ruckenstein (Sadeh), G. and Roth, R.M.	140
Effects of Finite-Precision Arithmetic in Enumerative Coding — Schouhamer Immink, K.A. and Janssen, A.	141
Power Spectral Density of Multitrack (0,G/I) Codes — Milenković, O. and Vasić, B.	142
Enumerative Huffman Coding — van der Walt, W. and Ferreira, H.C.	143
On the Construction of Constrained Codes Employing Sequence Replacement Techniques — van Wijngaarden, A.J. and Schouhamer Immink, K.A.	144
The Approximate Eigenvector Associated with a Modulation Code — Hollmann, H.D.L.	145
Session TUAM2 Communication for Fading Channels I	
Space-Time Codes for Wireless Communication — Calderbank, A.R., Seshadri, N., and Tarokh, V.	146
Decision Feedback MLD for CTDMA System — Wu, Y., Darnell, M., and Fan, P.	147
An Adaptive Projection Receiver for Asynchronous Coded CDMA — Schlegel, C., Alexander, P., and Roy, S.	148
Modeling and Undetected Error Performance of Diversity Channels — Swarts, F., Coetzee, C.S., and Ferreira, H.C.	149
A Broadcast Strategy for the Gaussian Slowly Fading Channel — Shamai (Shitz), S.	150
Performance of Joint Spatial and Temporal Multiuser Detection Using Adaptive Array Antenna in both Transmitter and Receiver for DS/CDMA — Kohno, R. and Ishii, N.	151
A Two-Stage SPRT-Based Acquisition Scheme for CDMA Wireless Communication Systems — Lin, J.-C. and Wei, C.-H.	152
Multiple-Antenna Transmission with Partial Side Information — Narula, A. and Trott, M.D.	153
Cooperative Signal Reception and Down-Link Beam Forming in Cellular Mobile Communications — Asakura, H. and Matsumoto, T.	154
Session TUAM3 Identification and Generation of Randomness	
On Maximum Number of Probability Measures on Finite Set Separated in L1 Metrics — Bassalygo, L.A. and Burnashev, M.V.	155
Identification of Messages and Identifying Zeroes of a Function — Kleinewaechter, C.	156
Common Randomness and Secret Key Generation with a Helper — Csiszár, I. and Narayan, P.	157
Random Number Generation with Cost by an Interval Algorithm — Hoshi, M. and Han, T.S.	158
Some Estimates of the Average Number of Guesses to Determine a Random Variable — Dragomir, S.S. and Boztas, S.	159
Elementary Forward Error Control for Identification Codes — van der Meulen, E.C. and Csibi, S.	160
Finite-Memory Hypothesis Testing with Semi-bounded Likelihood Ratio —	

Koplowitz, J. and Kulkarni, S.R.	161
Joint Source-Channel Coding and Guessing — Arikan, E. and Merhav, N.	162
Information Reconstruction Using Minimum Number of Erroneous Patterns and Optimization Problems of Multiple Transmission — Levenshtein, V.I.	163
Session TUAM4 Coded Modulation II	
Approaching the Capacity of the AWGN Channel with Coset Codes and Multilevel Coset Codes — Forney Jr., G.D.	164
Analysis of Power Density Spectra for Coded Modulation — Eier, R. and Kratochwil, K.	165
Trellis Code Construction for the Joint Source-Channel Problem — Belfiore, J.-C. and Guisantes, J.R. *	166
Performance of High Diversity Multidimensional Constellations — Taricco, G. and Viterbo, E.	167
Concordant and Partially Concordant Ring Convolutional Codes for CPFSK — Ugrelidze, N., Shavgulidze, S., and Chachua, L.	168
A New Signal Constellation for the Hierarchical Transmission of Two Equally Sized Data Streams — Seeger, A.	169
Block Coded Modulation Using Two-Level Group Codes over Generalized Quaternion Groups — Selvakumaran, T.V. and Sundar Rajan, B.	170
Block Coded Asymmetric PSK Modulation Using Two-Level Group Codes over Dihedral Groups — Bali, J. and Sundar Rajan, B.	171
Session TUAM5 Cryptology II	
Aspects of Authentication and Cryptology — Bäumer, L.	172
Codes Combining Error Detection and Authentication — Johansson, T.	173
Hash Codes — Bassalygo, L.A., Burmester, M., Dyachkov, A., and Kabatianskii, G.	174
Fast Authentication Codes Based on Random Polynomial Residue Classes — Afanassiev, V., Smeets, B., and Gehrman, C.	175
Large Deviations for Performance Analysis of Signature Authentication — O'Sullivan, J.A. and Ryleeva, N.	176
Large S-Box Design Using a Converging Method — Hendessi, F., Gulliver, T.A., and Sheikh, A.U.H.	177
Reconfigurable Feedback Shift Registers — Chan, A.H. and Médard, M.	178
An Algebraic Geometric Single Key Cryptosystem Using Stream Ciphers — Dawson, E. and Polemi, D.	179
Cryptographic Design Based on Cellular Automata — de la Guia-Martínez, D. and Fúster-Sabater, A.	180
Session TUAM6 Rate Distortion Theory	
Spectral Entropy, Equivalent Bandwidth and Minimum Coefficient Rate — Yang, W. and Gibson, J.D.	181
An Information-Spectrum Approach to Source Coding Theorems with a Fidelity Criterion — Han, T.S.	182
A Universal Data Compression with Common Side Information — Muramatsu, J. and Kanaya, F.	183
Fixed-Normal Lossy Lempel-Ziv Algorithm — Finomore, W.A. and Pinho, M.S.	184
A Simplistic, Universal Lossy Source Code — Neuhoff, D.L. and Shields, P.C.	185
A Type Generator Model for Adaptive Lossy Compression — Zamir, R. and Rose, K.	186
High-Resolution Source Coding for Non-Difference Distortion Measures: The Rate Distortion Function — Linder, T. and Zamir, R.	187
Complexity Distortion Theory — Sow, D. and Eleftheriadis, A.	188
Data Compression with Noise Suppression: A New Approach — Torokhti, A., Howlett, P., Moran, W., Gray, D., and Elhay, S.	189

Session TUAM7 Detection Theory I

A New Method for the Computation of Relative Efficiency (RE) of Detectors — Seyfe, B., Nikoofar, H.R., and Kahrizi, M.	190
Adaptive Reception in Impulsive Noise — Gonzalez, J.G., Griffith, D.W., Cooper III, A.B., and Arce, G.R.	191
Pipelined Sequential Probability Ratio Tests for Hybrid Serial Search — Hosangadi, G.S. and Baum, C.W.	192
Comparison of Several Receiver Structures for Trellis-Coded GMSK Signals: Analytical and Simulation Results — Tyczka, P. and Hołubowicz, W.	193
Aspects on Detection of Binary Signals on the Rayleigh Fading Channel — Hansson, U. and Aulin, T ...	194
Turbo-Based Multiuser Detection — Moher, M.L.	195
Weak-Signal Diversity Detection in Narrowband Non-Gaussian Noise — Izzo, L. and Tanda, M.	196
On the Equivalence of Single- and Multicarrier Modulation: A New View — Fischer, R.F.H. and Huber, J.B.	197
M. L. Estimation of Phase and Frequency of MPSK Signals — Taich, D. and Bar-David, I.	198

Session TUAM8 Codes over Z_4

Type II Codes over Z_4 — Bonnecaze, A., Solé, P., Bachoc, C., and Mourrain, B.	199
Cyclic Self-Dual Z_4 -Codes — Pless, V., Solé, P., and Qian, Z.	200
All Z_4 Codes of Type II and Length 16 are Known — Pless, V., Leon, J.S., and Fields, J.	201
All Self-Dual Z_4 Codes of Length 15 or Less are Known — Fields, J., Pless, V., and Leon, J.S.	202
Generalized Lee Weights for Codes over Z_4 — Hove, B.	203
On the Minimum Support Weights of Goethals Codes over Z_4 — Yang, K. and Helleseth, T.	204
On the Generalized Hamming Weights for Preparata Codes over Z_4 — Yang, K. and Helleseth, T.	205
Algebraic-Geometric Codes over Z_4 — Shanbhag, A.G. and Kumar, P.V.	206
Type II Self-Dual Codes over Finite Rings and Even Unimodular Lattices — Dougherty, S.T., Gulliver, T.A., and Harada, M.	207

Session TUPM1 Neural Networks & Game Theory

Convergence Analysis of Stochastic Pseudo-Gradient Algorithms and Application to Learning in Feedforward Neural Networks — Tadić, V. and Stanković, S.	208
Utilisation of an Adaptive Resonance Theory Neural Network as a Genetic Algorithm Fitness Evaluator — Burton, A.R. and Vladimirova, T.	209
Cantonese Phonemes Recognition using Modular Neural Network Approach — Hui, W.M., Liu, P.C.K., and Li, K.C.	210
State Clustering Method for Solving a Dynamic Jamming Game — Mallik, R.K.	211
Handwritten Numeral Recognition Using a Sequential Classifier — Lee, L.L. and Gomes, N.R.	212
New Improvements on the Real-Time Recurrent Learning Algorithm — Coelho, P.H.G.	213
On Grid Solutions of a Dynamic Jamming Game — Mallik, R.K. and Scholtz, R.A.	214
On Associative Nets — D'yachkov, A.G. and Rykov, V.V.	215

Session TUPM2 Recording & Line Codes II

Irreducible Components of Canonical Graphs for Second Order Spectral Nulls — Kamabe, H.	216
On Efficient m -ary Balanced Codes — Tallini, L.G. and Vaccaro, U.	217
Balanced and RLL Partial Unit Memory Codes — Markarian, G., Honary, B., and Thayananthan, V. ...	218

A Class of Low-Complexity Line Codes — Fragiocomo, S., Matrakidis, C., and O'Reilly, J.J.	219
A Method to Find Runlength Limited Block Error Control Codes — Fernandez, E.M.G. and Baldini F., R.	220
A Block Decodable Line Code for High Speed Optical Communication — Matrakidis, C. and O'Reilly, J.J.	221
On Achieving Frame Synchronization in Guided Scrambling Line Codes — Lampow-Maundy, H. and Fair, I.J.	222
On the Capacity Region of Write-Unidirectional Memory with Nonperiodic Codes — Fu, F.-W.	223
Session TUPM3 MAP and Iterative Decoding	
Map Tailbiting Decoders — Anderson, J.B. and Hladek, S.M.	224
On MAP Decoding for Tail-biting Convolutional Codes — Wang, Y.-P., Ramésh, R., Hassan, A., and Koorapaty, H.	225
Symbol-by-Symbol MAP Decoding of Convolutional Codes Using Reciprocal Dual Convolutional Codes — Riedel, S.	226
Turbo-Decoding of Nonbinary Codes — Berkmann, J. and Burkert, F.	227
Computationally Efficient Turbo Decoding with the Bi-Directional Viterbi Algorithm (BIVA) — Shoemake, M.B. and Heegard, C.	228
Optimum Soft Output MAP Detector for Coded Multiuser Communications — Vojcic, B.R., Shama, Y., and Pickholtz, R.L.	229
Reduced-Search BCJR Algorithms — Franz, V. and Anderson, J.B.	230
Soft Decision MAP Decoding of Binary Linear Block Codes via Global Optimization — Schäffler, S. and Hagenauer, J.	231
Belief Propagation in Loopy Bayesian Networks: Experimental Results — Horn, G.B. and McEliece, R.J.	232
Session TUPM4 Communication for Fading Channels II	
New Insight into the Performance of TCM Schemes over Fast Time-Variant Multipath-Degraded Faded Environments — Baccarelli, E., Cusani, R., and Galli, S.	233
Results on Code Design for Transmitter Diversity in Fading — Fitz, M.P., Grimm, J., and Krogmeier, J.V.	234
Trellis Codes for Time-Selective Rician-Fading Channels — Noneaker, D.L. and Frank, C.	235
Analysis of Frequency-Hopped Spread-Spectrum Multiple-Access with M -ary FSK over a Rayleigh Fading Channel — Wilhelmsson, L. and Zigangirov, K.Sh.	236
A Combined Adaptive Equalizer and TCM-Decoder for Fast Time-Variant ISI-Degraded Rayleigh Radio Channels — Baccarelli, E., Cusani, R., Di Blasio, G., and Galli, S.	237
Cutoff Rate Performance for Space Diversity Systems in a Correlated Rayleigh Fading Channel with CSI — Ohtsuki, T.	238
The Performance of GMSK in Fading and Co- and Adjacent Channel Interference Using the Exact Interference Distributions — Vigneron, P.J. and Wittke, P.H.	239
Error Exponents for Two-Dimensional Time Correlated Flat Fading Channels with Space Diversity and Channel Estimation — Ahmed, W.K.M. and McLane, P.J.	240
Acquisition-Based Capacity of a DS/CDMA System with Imperfect Power Control in a Nakagami Fading Channel — Kim, J.Y. and Lee, J.H.	241

Session TUPM5 Synchronization & Signal Processing

Minimum Energy in Information Transmission — Levitin, L.B.	242
Moving Average Restoration of Band-Limited Signals from Noisy Observations — Krzyżak, A., Rafajłowicz, E., and Pawlak, M.	243
Irregular Sampling Theorems for Wavelet Subspaces — Chen, W., Itoh, S., and Shiki, J.	244
On the Asymptotic Behavior of Recursive Maximum Likelihood Estimation for Symbol Timing Recovery over AWGN Channels — Lu, C.-C. and Wang, W.-S.	245
I and Q Decomposition of Self Noise in a Clock Recovery System Employing a General Type of Nonlinearity — Panayırıcı, E.	246
A Chaos Model of Finite-Order Markov Sources and Arithmetic Coding — Kanaya, F.	247
Metrics Generated by a Projective Point Set — Gabidulin, E.M. and Simonis, J.	248
A Tight Upper Bound on Discrete Entropy — Mow, W.H.	249

Session TUPM6 Algebraic Coding Theory I

Optimized Arithmetic for Reed-Solomon Encoders — Paar, C.	250
The Average Binary Expansion of a Reed-Solomon Code is Good for Error Detection — Rettter, C.T.	251
Linear Codes and the Two-Way Chain Condition — Encheva, S.B.	252
Many Non-Abelian Groups Support Only Group Codes That are Conformant to Abelian Group Codes — Massey, P.C.	253
Cyclic Subcodes of Generalized Reed-Muller Codes — Moreno, O., Duursma, I.M., Cherdieu, J.P., and Edouard, A.	254
The Diametric Theorem in Hamming Spaces – Optimal Anticodes — Ahlswede, R. and Khachatrian, L.H.	255
Code Pairs with Specified Parity of the Hamming Distances — Ahlswede, R. and Zhang, Z.	256
Some New Circuit Codes — Paterson, K.G. and Tuliani, J.	257
Block Coding Based on a Tree Classifier — Huang, J. and Zhang, L.	258

Session TUPM7 Error Correcting Techniques

Reed-Solomon Codes Meet the Error Exponent of the Asymptotic Uniform Symmetric Channel — Lazic, D.E. and Beth, Th.	259
New Double-Byte Error-Correcting Codes for Memory Systems — Feng, G.-L., Wu, X. and Rao, T.R.N.	260
Improved EVENODD Code — Feng, D., Jin, H., and Zhang, J.	261
Error Propagation in Protocol Stacks — Zorzi, M. and Rao, R.R.	262
Subfield Checking in BCH-Decoding — Tolhuizen, L.	263
Metrics of Error Locating Codes — Kitakami, M., Jiang, S., and Fujiwara, E.	264
Multilevel Diversity Coding via Successive Refinement — Zamir, R. and Yeung, R.	265
Conditions on the Optimality of Multilevel Codes — Wachsmann, U. and Huber, J.B.	266

Session TUPM8 Multi-User Channels and Sources

An Outer Bound for E-Capacity Region of Broadcast Channel Giving a New Outer Bound for Capacity Region — Haroutunian, M.E. and Haroutunian, E.A.	267
A Framework for Information Inequalities — Yeung, R.W.	268
Körner-Marton's Zig-Zag Problem for Correlated Memoryless Gaussian Sources — Oohama, Y.	269
Achieving Vertices of the Capacity Region of the Synchronous Gaussian Correlated-Waveform Multiple-Access Channel with Decision-Feedback Receivers — Varanasi, M.K. and Guess, T.	270

Asynchronous Slepian-Wolf Coding via Source-Splitting — Rimoldi, B. and Urbanke, R.	271
Sequential Coding of Correlated Sources — Viswanathan, H. and Berger, T.	272
Multiple Description Source Encoding of a Gaussian Random Variable: A Geometric Treatment — Batllo, J.-C. and Vaishampayan, V.A.	273
Source Coding Theorem for an Extended Slepian-Wolf System with Two Interactive Decoders — Yamamoto, H.	274
Asymptotically Optimum Multiuser Decision Feedback Detection — Varanasi, M.K.	275
Session WEAM1 Shannon Theory	
Multilevel Distributed Source Coding — Yeung, R.W. and Zhang, Z.	276
Maximizing the Entropy of a Sum of Independent Random Variables — Ordentlich, E.	277
Is Maximum Entropy Noise the Worst? — Diggavi, S.N. and Cover, T.M.	278
On a Problem about I-Projections — Csiszár, I. and Finesso, L.	279
Convex Duality and the Value of Side Information — Algoet, P.	280
Asymptotically Optimum Selections in Convex Families — Algoet, P.	281
The Equivalence of Optimal Market Gain and Minimax Regret Universal Portfolios — Cover, T. and Ordentlich, E.	282
The Initial Efficiency of Investment for the General Market — Erkip, E. and Cover, T.M.	283
Session WEAM2 Convolutional Codes	
Some Results on Convolutional Codes over Rings — Johannesson, R., Wan, Z., and Wittenmark, E.	284
Convolutional Codes over Rings and the Two Chain Conditions — Mittelholzer, T.	285
Trellis-Canonical Generator Matrices for Convolutional Codes — Lin, W., McEliece, R.J., and Xu, M.	286
Analyzing Convolutional Encoders Using Realization Theory — Allen, B.M. and Rosenthal, J.	287
Determination of Inverses and Syndrome Formers for 2-D Convolutional Encoders — Koorapaty, H., Dholakia, A., Bitzer, D.L., and Vouk, M.A.	288
How to Determine Cosets of Convolutional Codes with Least Possible Maximum Zero-Run Lengths — Hole, K.J. and Ytrehus, Ø.	289
Convolutional Codes for Unequal Error Protection — Chiu, M.-C., Chao, C.-c., and Wang, C.-H.	290
A Construction of Binary BCH Convolutional Codes — Rosenthal, J. and York, E.V.	291
Session WEAM3 Algebraic Coding Theory II	
Quantum Error Correction Via Codes over GF(4) — Calderbank, A.R., Rains, E.M., Shor, P.W., and Sloane, N.J.A.	292
Universal Codes and Unimodular Lattices — Chapman, R. and Solé, P.	293
On Adjacent Asymmetric Error Masking (AAEM) Codes — Tallini, L.G. and Bose, B.	294
New Commutative Group Codes — Pellenz, M.E. and Portugheis, J.	295
Array Codes with Progressive Redundancy — Roth, R.M. and Seroussi, G.	296
On the Design of t -EC/AUED Codes — Yang, C.-N. and Laih, C.-S.	297
Nonexistence Results for Spherical 3-Designs of Small Cardinalities — Boyvalenkov, P., Nikova, S., and Nikov, V.	298
One Generalization of Goppa Codes — Bezzateev, S.V. and Shekhunova, N.A.	299