

2006 IEEE Information Theory Workshop

13 – 17 March 2006

Punta del Este, Uruguay

Copyright © 2006 Institute of Electrical and Electronics Engineers, Inc.

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 first 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 Operations Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331. All rights reserved.

IEEE Catalog Number: 06EX1253

ISBN: 1-4244-0035-X

Library of Congress Number: 2005936277

TABLE OF CONTENTS

Shannon theory	
Lautum information	1
<i>Daniel P. Palomar, Sergio Verdú</i>	
Reliable communication over an optical fading channel	6
<i>Kaushik Chakraborty, Prakash Narayan</i>	
Coding for channels with rate-limited side information at the decoder	11
<i>Yossef Steinberg</i>	
Delay-limited OFDM broadcast capacity region and impact of system parameters	14
<i>Gerhard Wunder, Thomas Michel</i>	
 Cryptography and data security	
A promenade through the new cryptography of bilinear pairings	19
<i>Xavier Boyen</i>	
Oblivious transfer and quantum channels	24
<i>Nicolas Gisin, Sandu Popescu, Valerio Scarani, Stefan Wolf, Jürg Wullschlegler</i>	
Inverting bijective polynomial maps over finite fields	27
<i>Antonio Cafure, Guillermo Matera, Ariel Waissbein</i>	
 Recent trends in algebraic and combinatorial coding theory	
List decoding in average-case complexity and pseudorandomness	32
<i>Venkatesan Guruswami</i>	
On optimal weight assignments for multivariate interpolation list-decoding	37
<i>Ralf Koetter</i>	
Fidelity of a quantum ARQ protocol	42
<i>Alexei Ashikhmin</i>	
Perfect codes in the Johnson schemes	47
<i>Tuvi Etzion</i>	
 Data networks	
Layering as optimization decomposition: framework and examples	52
<i>Mung Chiang, Steven H. Low, A. Robert Calderbank, John C. Doyle</i>	
Equilibrium of heterogeneous congestion control protocols	57
<i>Ao Tang, Jiantao Wang, Steven Low, Mung Chiang</i>	
A tiling approach to network code design for wireless networks	62
<i>Michelle Effros, Tracey Ho, Sukwon Kim</i>	
Fast gossip via non-reversible random walk	67
<i>Kyomin Jung, Devavrat Shah</i>	
 On-line algorithms and learning	
Regret minimization under partial monitoring	72
<i>Nicolò Cesa-Bianchi, Gábor Lugosi, Gilles Stoltz</i>	
Compound sequential decisions against the well-informed antagonist	77
<i>Tsachy Weissman</i>	
Calibration via regression	82
<i>Dean P. Foster, Sham M. Kakade</i>	
The shortest path problem in the bandit setting	87
<i>András György, Tamás Linder, Gábor Lugosi</i>	
 Analysis of algorithms in information theory / Applications of finite fields	
Compressing with collapsible tries	92
<i>Alberto Apostolico, Yong Wook Choi</i>	
Control of mobile ad hoc networks	97
<i>Philippe Jacquet</i>	
Statistics for dynamical sources	102
<i>Brigitte Vallée</i>	

Fast arithmetic for polynomials over F_2 in hardware	107
<i>Joachim von zur Gathen, Jamshid Shokrollahi</i>	
Some results on codes over Galois rings	112
<i>Horacio Tapia-Recillas</i>	
Cryptography	
LDPC-based Gaussian key reconciliation	116
<i>Mathieu Bloch, Andrew Thangaraj, Steven W. McLaughlin, Jean-Marc Merolla</i>	
Families of traceability codes based on the Chinese Remainder Theorem	121
<i>Josep Cotrina, Marcel Fernandez, Jordi Casademont</i>	
New point compression algorithms for binary curves	126
<i>Julio López, Ricardo Dahab</i>	
Source coding	
Tight bounds on the redundancy of Huffman codes	131
<i>Soheil Mohajer, Payam Pakzad, Ali Kakhbod</i>	
Distortion exponent of MIMO fading channels	136
<i>Deniz Gunduz, Elza Erkip</i>	
Successive refinement for pattern recognition	141
<i>Joseph A. O'Sullivan, Naveen Singla, M. Brandon Westover</i>	
Coding techniques for storage and other applications	
On coding for 2-D storage systems	146
<i>Jack Keil Wolf</i>	
On the probability of undetected error for over-extended Reed-Solomon codes	150
<i>Junsheng Han, Paul H. Siegel, Patrick Lee</i>	
Punctured vs rateless codes for hybrid ARQ	155
<i>Emina Soljanin, Nedeljko Varnica, Philip Whiting</i>	
LDPC codes, Turbo codes, and iterative decoding	
Analysis of belief propagation for non-linear problems: the example of CDMA (or: how to prove Tanaka's formula)	160
<i>Andrea Montanari, David Tse</i>	
Design principles for Raptor codes	165
<i>Payam Pakzad, Amin Shokrollahi</i>	
Some graph products and their expansion properties	170
<i>Andrew Brown, Amin Shokrollahi</i>	
Bounds on the threshold of linear programming decoding	175
<i>Pascal O. Vontobel, Ralf Koetter</i>	
Using many machines to handle an enormous error-correcting code	180
<i>Jon Feldman</i>	
A new fast density evolution	183
<i>Hui Jin, Tom Richardson</i>	
On the design of S-type permutors for double serially concatenated convolutional codes	188
<i>Axel Huebner, Daniel J. Costello, Jr</i>	
Multi-user information theory	
Iterative and one-shot conferencing in relay channels	193
<i>Chris T. K. Ng, Ivana Maric, Andrea J. Goldsmith, Shlomo Shamai (Shitz), Roy D. Yates</i>	
Dependence balance and the gaussian multiaccess channel with feedback	198
<i>Gerhard Kramer, Michael Gastpar</i>	
A simple derivation of Burnashev's reliability function	203
<i>Peter Berlin, Bixio Rimoldi, Emre Telatar</i>	
Backward channels in multiterminal source coding	206
<i>Sergio D. Servetto</i>	
Algebraic and combinatorial aspects of information theory	
On the coding advantage of multiple unicast sessions in undirected graphs	211
<i>Kamal Jain, Vijay V. Vazirani, Gideon Yuval</i>	

Another diametric theorem in Hamming spaces: optimal group anticodes.	212
<i>Rudolf Ahlswede</i>	
Approximating the number of differences between remote sets	217
<i>Sachin Agarwal, Ari Trachtenberg</i>	
Superposition by position.	222
<i>Hui Jin, Rajiv Laroia, Tom Richardson</i>	
Universal schemes	
On opportunistic codes and broadcast codes with degraded message sets	227
<i>Suhas N. Diggavi, David N C. Tse</i>	
On context-tree prediction of individual sequences.	232
<i>Jacob Ziv, Neri Merhav</i>	
Online learning with universal model and predictor classes	237
<i>Jan Poland</i>	
Theoretical and experimental results on modeling low probabilities	242
<i>Alon Orlitsky, Narayana Santhanam, Krishnamurthy Viswanathan, Junan Zhang</i>	
Data compression	
A partial solution for lossless source coding with coded side information.	247
<i>Daniel Marco, Michelle Effros</i>	
The error exponent with delay for lossless source coding.	252
<i>Cheng Chang, Anant Sahai</i>	
Entropy estimation: simulation, theory and a case study.	257
<i>Ioannis Kontoyiannis</i>	
On the significance of binning in a scaling-law sense.	258
<i>Krishnan Eswaran, Michael Gastpar</i>	
Low-density constructions for lossy compression, binning, and coding with side information.	263
<i>Emin Martinian, Martin J. Wainwright</i>	
Coding theory	
On hybrid ARQ protocol schemes over the $m(\geq 2)$ -ary asymmetric channel	265
<i>Luca G. Tallini, Samir Elmougy, Bella Bose</i>	
Code synchronization, cyclotomy, and finite geometry.	270
<i>Vladimir D. Tonchev</i>	
Upper bounds for a commutative group code	275
<i>Rogério Monteiro de Siqueira, Sueli I. Rodrigues Costa</i>	
On a new q -ary combinatorial analog of the binary Grey-Rankin bound and codes meeting this bound	278
<i>Leonid Bassalygo, Stefan Dodunekov, Tor Helleseht, Victor Zinoviev</i>	
On the behavior of the distance spectrum of convolutional codes under a minimal trellis complexity measure.	283
<i>Bartolomeu F. Uchôa-Filho, Richard Demo Souza, Cecilio Pimentel</i>	
Multi-user information theory II	
The role of SNR in achieving MIMO rates in cooperative Systems.	288
<i>Chris T. K. Ng, J. Nicholas Laneman, Andrea J. Goldsmith</i>	
Linear multiuser detection for asynchronous CDMA systems: chip pulse design and time delay distribution	293
<i>Laura Cottatellucci, Mérouane Debbah, Ralf R. Müller</i>	
Scaling law of the sum-rate for multi-antenna broadcast channels with deterministic or selective binary feedback.	298
<i>Jordi Diaz, Osvaldo Simeone, Oren Somekh, Yeheskel Bar-Ness</i>	
On the capacity of small-world networks	302
<i>Rui A. Costa, João Barros</i>	
Network coding in minimal multicast networks	307
<i>Salim Y. El Rouayheb, Costas N. Georghiades, Alexander Sprintson</i>	
LDPC codes and serially concatenated codes / Space-time codes	
On the relation between MAP and BP GEXIT functions of low density parity check codes.	312
<i>Nicolas Macris</i>	
The block error probability of detailedly represented irregular LDPC code ensembles under maximum likelihood decoding.	317
<i>Ryoji Ikegaya, Kenta Kasai, Tomoharu Shibuya, Kohichi Sakaniwa</i>	

A new tool: constructing STBCs from maximal orders in central simple algebras	322
<i>Camilla Hollanti, Jyrki Lahtonen</i>	
Novel unitary space-time signal design	327
<i>David B. Smith, Leif W. Hanlen</i>	
Pattern recognition and learning / Information theory and statistics	
Distributed kernel regression: an algorithm for training collaboratively.	332
<i>Joel B. Predd, Sanjeev R. Kulkarni, H. Vincent Poor</i>	
Bayesian model selection for independent factor analysis	337
<i>Omolabake A. Adenle, William J. Fitzgerald</i>	
Random series in $L_p(X, S, m)$ using unconditional basic sequences: a result on almost sure almost everywhere convergence.	342
<i>Juan Miguel Medina, Bruno Cernuschi Frías</i>	
Non-coherent mutual information of the multipath Rayleigh fading channel in the low SNR regime	345
<i>Lei Zhou, Shidong Zhou, Yan Yao</i>	
Keynote lectures	
Combinatorial games	350
<i>Elwyn Berlekamp</i>	
Information and Complexity in Statistical Modeling.	351
<i>Jorma Rissanen</i>	