2010 IEEE Information Theory Workshop

(ITW 2010)

Dublin, Ireland
30 August – 3 September 2010
# TABLE OF CONTENTS

**PLENARY TALK:**

Abelian Varieties in Coding and Cryptography

I. F. Blake

**CODING AND INFORMATION-THEORETIC METHODS IN CRYPTOGRAPHY:**

Recent Results on Bent and Hyper-bent Functions and Their Link With Some Exponential Sums

Sihem Mesnager

Boolean Functions Whose Restrictions are Highly Nonlinear

Constanza Riera, Matthew G. Parker

Hecke Operators with odd Determinant and Binary Frameproof Codes

Beyond the Probabilistic Bound?

Hugues Randriam

Robust Parent-identifying Codes

Alexander Barg, G. Robert Blakley, Grigory Kabatiansky, Cedric Tavernier

Coding Solutions for the Secure Biometric Storage Problem

Davide Schipani, Joachim Rosenthal

Identification Codes in Cryptographic Protocols

Julien Bringer, Herve Chabanne, Gerard Cohen, Bruno Kondarji

**COOPERATION AND THROUGHPUT IN NETWORKS:**

Cooperative Strategies for Relay-Aided Multi-Cell Wireless Networks with Backhaul

Jinfeng Du, Ming Xiao, Mikael Skoglund

Throughput and Latency of Acyclic Erasure Networks with Feedback in a Finite Buffer Regime

Nima Torabkhani, Badri N. Vellambi, Faramarz Fekri

Cooperative ARQs with Opportunistic Distributed Space-time Coding: Effective Protocols and Performance Analysis

Hsin-Li Chiu, Sau-Hsuan Wu, Jin-Hao Li

On the Deterministic Multicast Capacity of Bidirectional Relay Networks

M. Mokhtar, Y. Mohasseb, M. Nafie, H. El Gamal

**LOW-DENSITY CODES:**

Structured LDPC Codes from Permutation Matrices Free of Small Trapping Sets

Dung Viet Nguyen, Bane Vasic, Michael Marcellin, Shashi Kiran Chilappagari

Quasi-cyclic Asymptotically Regular LDPC Codes

David G. M. Mitchell, Roxana Smarandache, Michael Lentmaier, Daniel J. Costello

Irregular Repeat-accumulate-like Codes with Improved Error Floor Performance

David F. Hayes, Sarah J. Johnson, Steven R. Weller

Lossy Source Compression of Non-uniform Binary Sources Using GQ-LDGM Codes

Lorenzo Cappellari

**COMMUNICATION WITH SECRECY SONCTRAINTS:**

Strong Secrecy for Erasure Wiretap Channels

Ananda T. Suresh, Arunkumar Subramanian, Andrew Thangaraj, Matthieu Bloch, Steven W. McLaughlin

Wiretap Channel with Shared Key

Wei Kang, Nan Liu

Multiple Access Wiretap Channels with Strong Secrecy

Mohammad Hossein Yassae, Mohammad Reza Aref
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Speed of Channel Polarization</td>
<td>189</td>
</tr>
<tr>
<td>Toshiyuki Tanaka</td>
<td></td>
</tr>
<tr>
<td><strong>POLAR AND LDPC CODES:</strong></td>
<td></td>
</tr>
<tr>
<td>Polar Coding for Reliable Communications over Parallel Channels</td>
<td>194</td>
</tr>
<tr>
<td>Eran Hof, Igal Sason, Shlomo Shamai</td>
<td></td>
</tr>
<tr>
<td>Non-binary Polar Codes using Reed-solomon Codes and Algebraic Geometry Codes</td>
<td>199</td>
</tr>
<tr>
<td>Ryuhei Mori, Toshiyuki Tanaka</td>
<td></td>
</tr>
<tr>
<td>On LP Decoding of Polar Codes</td>
<td>204</td>
</tr>
<tr>
<td>Naveen Goela, Satish Babu Korada, Michael Gastpar</td>
<td></td>
</tr>
<tr>
<td><strong>COMMUNICATION THEORY 2:</strong></td>
<td></td>
</tr>
<tr>
<td>On the Capacity Region of the Degraded Z Channel</td>
<td>209</td>
</tr>
<tr>
<td>Sadaf Salehkalaibar, Mohammad Reza Aref</td>
<td></td>
</tr>
<tr>
<td>Bit-interleaved Coded Modulation with Shaping</td>
<td>214</td>
</tr>
<tr>
<td>Albert Guillen I. Fabregas, Alfonso Martinez</td>
<td></td>
</tr>
<tr>
<td>Achievable Rate Regions for Dirty Tape Channels and &quot;Joint Writing on Dirty Paper and Dirty Tape&quot;</td>
<td>219</td>
</tr>
<tr>
<td>Reza Khosravi-Farsani, Bahareh Akhbari, Mohammad Reza Aref</td>
<td></td>
</tr>
<tr>
<td>Coding for the Z Channel With a Digital Relay Link</td>
<td>224</td>
</tr>
<tr>
<td>Hieu T. Do, Tobias J. Oechtering, Mikael Skoglund</td>
<td></td>
</tr>
<tr>
<td><strong>ALGEBRAIC CODES:</strong></td>
<td></td>
</tr>
<tr>
<td>On the Degree of the Inverse of Quadratic Permutation Polynomial Interleavers</td>
<td>229</td>
</tr>
<tr>
<td>Eeva Suvitie, Jyrki Lahtonen</td>
<td></td>
</tr>
<tr>
<td>The Projective Kerdock Code</td>
<td>234</td>
</tr>
<tr>
<td>M. M. Nastasescu, A. R. Calderbank</td>
<td></td>
</tr>
<tr>
<td>Information sets for Abelian Codes</td>
<td>239</td>
</tr>
<tr>
<td>Jose Joaquin Bernal, Juan Jacobo Simon</td>
<td></td>
</tr>
<tr>
<td>Additive Codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$</td>
<td>244</td>
</tr>
<tr>
<td>Joaquim Borges, Cristina Fernandez-Cordoba, Steven T. Dougherty</td>
<td></td>
</tr>
<tr>
<td><strong>GRAPHICAL MODELS AND DECODING:</strong></td>
<td></td>
</tr>
<tr>
<td>Tail-biting Products Trellises, the BCJR-construction and their Duals</td>
<td>247</td>
</tr>
<tr>
<td>Heide Gluesing-Luerssen, Elizabeth Weaver</td>
<td></td>
</tr>
<tr>
<td>Valiant Transform of Forney Graphs</td>
<td>252</td>
</tr>
<tr>
<td>Ali Al-Bashabsheh, Yongyi Mao</td>
<td></td>
</tr>
<tr>
<td>An Algebraic View to Gradient Descent Decoding</td>
<td>257</td>
</tr>
<tr>
<td>M. Borges Quintana, M. A. Borges Trenard, I. Marquez-Corbella, E. Martinez-Moro</td>
<td></td>
</tr>
<tr>
<td>The Euclidean Algorithm for Generalized Minimum Distance Decoding of Reed-solomon Codes</td>
<td>261</td>
</tr>
<tr>
<td>Sabine Kampf, Martin Bossert</td>
<td></td>
</tr>
<tr>
<td>Universal A Posteriori Metrics Game</td>
<td>266</td>
</tr>
<tr>
<td>Emmanuel Abbe, Retnakaran Pulikkoonattu</td>
<td></td>
</tr>
<tr>
<td><strong>CODING AND DECODING:</strong></td>
<td></td>
</tr>
<tr>
<td>Computation of the Robust Symmetrical Number System Dynamic Range</td>
<td>271</td>
</tr>
<tr>
<td>Brian L. Luke, Phillip E. Pace</td>
<td></td>
</tr>
<tr>
<td>Properties of Optimal Prefix-free Machines as Instantaneous Codes</td>
<td>276</td>
</tr>
<tr>
<td>Kohtaro Tadaki</td>
<td></td>
</tr>
<tr>
<td>Group Permutable Constant Weight Codes</td>
<td>281</td>
</tr>
<tr>
<td>Oscar Moreno, Jose Ortiz-Ubarri</td>
<td></td>
</tr>
</tbody>
</table>
Codes from Graphs Related to the Categorical Product of Triangular Graphs and $K_n$ ................................. 286
Khumbo Kumwenda, Eric Mwambene

INTERFERENCE CHANNELS:

On Achievable Rates for Classes of Non-linear Deterministic Interference Channels ........................................... 291
Amin Jafarian, Sriram Vishwanath

Outer Bounds for the Interference Channel with a Cognitive Relay ................................................................. 296
Stefano Rini, Daniela Tuninetti, Natasha Devroye

Capacity Regions for Some Classes of Causal Cognitive Interference Channels With Delay .................................. 301
Mahatab Mirmohseni, Bahareh Akhbari, Mohammad Reza Aref

Sum Capacity of $K$ User Gaussian Degraded Interference Channels .......................................................... 306
Jubin Jose, Sriram Vishwanath

The Capacity Region of the Interference Channel with a Relay in the Strong Interference Regime
Subject to Phase Fading ........................................................................................................................................... 311
Ron Dabora

PLENARY TALK:

Local Computation in Codes .................................................................................................................................. 316
Tali Kaufman

LDPC CODES:

Improved Linear Programming Decoding and Bounds on the Minimum Distance of LDPC Codes ................ 321
David Burshtein, Idan Goldenberg

A Graphical Model for Computing the Minimum Cost Transposition Distance .................................................. 326
Farzad Farnoud, Chien-Yu Chen, Olgica Milenkovic, Navin Kashyap

Coupled Graphical Models and their Thresholds ........................................................................................................... 331
S. Hamed Hassani, Nicolas Macris, Ruediger Urbanke

Characterization of Graph-cover Pseudocodewords of Codes over $F_3$ .......................................................... 336
Vitaly Skachek

WIRELESS NETWORKS:

Network-level Cooperative Protocols for Wireless Multicasting: Stable Throughput
Analysis and Use of Network Coding ....................................................................................................................... 341
Anthony Fanous, Anthony Ephremides

The Benefits from Simultaneous Transmission and Reception in Wireless Networks ......................................... 346
P. C. Weeraddana, M. Codreanu, M. Latva-aho, Anthony Ephremides

The Collection Channel In a Wireless Sensor Network .......................................................................................... 351
Bryan Larish, George Riley

Fireworks: A Random Linear Coding Scheme for Distributed Storage in Wireless Sensor Networks ............. 356
Dejan Vukobratovic, Cedomir Stefanovic, Vladimir Stankovic

ALGEBRAIC CODES AND SEQUENCES:

Unimodular Lattices for the Gaussian Wiretap Channel ......................................................................................... 361
Jean-Claude Belfiore, Patrick Solé

Generalized Frobenius Extensions of Finite Rings and Trace Functions ............................................................ 366
Marcus Greferath, Alexandr Nechaev

The Enumeration of Costas Arrays of Order 28 ...................................................................................................... 371
Konstantinos Drakakis, Francesco Iorio, Scott Rickard
ESTIMATION AND PORTFOLIO THEORY:

The Confidence Interval of Entropy Estimation through a Noisy Channel .................................................. 376
Siu-Wai Ho, Terence Chan, Alex Grant

On Conditions for Linearity of Optimal Estimation ....................................................................................... 381
Emrah Akyol, Kumar Viswanatha, Kenneth Rose

On Thresholds for Robust Goodness-of-fit Tests ......................................................................................... 386
Jayakrishnan Unnikrishnan, Sean Meyn, Venugopal V. Veeravalli

Universal Portfolio Algorithms in Realistic-outcome Markets .................................................................... 390
Ami Tavory, Meir Feder

INFORMATION THEORETIC METHODS:

Error Exponents in Multiple Hypothesis Testing for Arbitrarily Varying Sources...................................... 395
Naira M. Grigoryan, Ashot N. Harutyunyan

Capacity of a Noisy Function ......................................................................................................................... 400
Francois Simon

Source Coding With Common Reconstruction and Action-dependent Side Information ............................ 405
Kittipong Kittichokechai, Tobias J. Oechtering, Mikael Skoglund

Information-theoretical Analysis of Private Content Identification ............................................................. 410
S. Voloshynovskiy, O. Koval, F. Beekhof, F. Farhadiadeh, T. Holotyak

QUANTUM INFORMATION PROCESSING:

Quantum Channel Capacities .......................................................................................................................... 415
Graeme Smith

Stabilizer Subsystem Codes with Spatially Local Generators ........................................................................ 420
Sergey Bravyi

Quantum Erasure-correcting Codes and Percolation on Regular Tilings of the Hyperbolic Plane .............. 425
Nicolas Delfosse, Gilles Zemor

NETWORK CODING:

Rotate-and-add Coding: A Novel Algebraic Network Coding Scheme ......................................................... 430
Alireza Keshavarz-Haddad, Mohammad Amir Khojastepour

On the Delay Advantage of Coding in Packet Erasure Networks ............................................................ 435
Theodosis K. Dikaliotis, Alexandros Dimakis, Tracey Ho, Michelle Effros

Orbit Codes - A New Concept in the Area of Network Coding .................................................................. 440
Anna-Lena Trautmann, Felice Manganiello, Joachim Rosenthal

On Secure Network Coding with Unequal Link Capacities and Restricted Wiretapping Sets .................. 444
Tao Cui, Tracey Ho, Joerg Kliewer

QUANTUM INFORMATION PROCESSING (CON'D):

On Encoders for Quantum Convolutional Codes ........................................................................................... 449
Markus Grassl, Martin Roetteler

A Renormalization Group Decoding Algorithm for Topological Quantum Codes ..................................... 454
Guillaume Duclos-Cianci, David Poulin

Topological Color Codes over Higher Alphabet ........................................................................................... 459
Pradeep Sarvepalli

CODING AND CAPACITY OF NETWORKS:

Multi-source Operator Channels: Efficient Capacity-achieving Codes ....................................................... 464
Hongyi Yao, Theodosis K. Dikaliotis, Sidharth Jaggi, Tracey Ho

Reduced-state Decoding in Two-way Relay Networks With Physical-layer Network Coding .................. 469
Duc To, Jinho Choi
Approximate Capacity of a Class of Multi-source Gaussian Relay Networks .......................................................... 474
Sang-Woon Jeon, Sae-Young Chung, Syed A. Jafar

Gaussian Diamond Network with Adversarial Jammer ................................................................................................. 479
Soheil Mohajer, Suhas N. Diggavi

PLENARY TALK:

Applications of Semidefinite Programming to Coding Theory ................................................................. 484
Christine Bachoc

CHANNEL UNCERTAINTY:

Every Channel with Time Structure has a Capacity Sequence ........................................................................... 489
Rudolf Ahlswede

Coding Against Myopic Adversaries ..................................................................................................................... 490
Anand D. Sarwate

A Multi-hop Multi-source Algebraic Watchdog .................................................................................................. 495
MinJi Kim, Muriel Medard, Joao Barros

Author Index