

2011 IEEE Information Theory Workshop

(ITW 2011)

**Paraty, Brazil
16 – 20 October 2011**



**IEEE Catalog Number: CFP11IFO-PRT
ISBN: 978-1-4577-0438-3**

Program

Sunday, October 16

Opening ceremony - Welcome cocktail

Monday, October 17

P1: Plenary Talk: Recent Advances in Sphere Packing - Neil J. A. Sloane

I1A: Invited Session I: Coding Theory

Organizer: Frédérique Oggier

Lattice Codes for the Compute-and-Forward Protocol: The Flatness Factor

J. C. Belfiore
pp. 1-4

Flip-OFDM for Optical Wireless Communications

N. Fernando, Yi Hong and E. Viterbo
pp. 5-9

Generalized Distributive Law for ML Decoding of STBCs

L. P. Natarajan, P. Srinath and B. S. Rajan
pp. 10-14

I1B: Invited Session II: Compressed Sensing

Organizer: Olgica Milenkovic

Approaching the Capacity of Sampled Analog Channels

Y. Chen, Y. Eldar and A. Goldsmith
pp. 15-19

Symmetric Group Testing and Superimposed Codes

A. Emad and O. Milenkovic
pp. 20-24

Nesterov's method in compressive sensing

A. Nedich

Coffee Break

S1A: Coding Theory and Practice I

An Algorithmic Approach for Finding Deletion Correcting Codes

F. Khajouei, M. Zolghadr and N. Kiyavash
pp. 25-29

Self-Repairing Codes for Distributed Storage --- A Projective Geometric Construction

F. Oggier and A. Datta
pp. 30-34

The Expected Write Deficiency of Index-Less Flash Codes and Their Improvement

Y. Kaji
pp. 35-39

Non-binary WOM-Codes for Multilevel Flash Memories

R. Gabrys, E. Yaakobi, L. Dolecek, P. Siegel, A. Vardy and J. Wolf
pp. 40-44

Quasicyclic MDS Codes for Distributed Storage with Efficient Exact Repair

A. Thangaraj and C. Sankar
pp. 45-49

S1B: Physical-layer Security I

Embedding Information Flows into Renewal Traffic

S. Marano, V. Matta, T. He and L. Tong
pp. 50-54

Non-Malleable Codes from the Wire-Tap Channel

H. Chabanne, G. Cohen, J. P. Flori and A. Patey
pp. 55-59

Capacity results for compound wiretap channels

I. Bjelaković, H. Boche and J. Sommerfeld
pp. 60-64

Secret Message Capacity of Erasure Broadcast Channels with Feedback

L. Czap, V. Prabhakaran, C. Fragouli and S. Diggavi
pp. 65-69

Secrecy Gain of Trellis Codes: The Other Side of the Union Bound

Y. Yan, C. Ling and J. C. Belfiore
pp. 70-74

S1C: Information Theory in Biology

On Multiple Hypothesis Testing with Rejection Option

N. Grigoryan, A. Harutyunyan, S. Voloshynovskiy and O. Koval
pp. 75-79

Exponential Pattern Retrieval Capacity with Non-Binary Associative Memory

K. R. Kumar, A. H. Salavati and A. Shokrollahi
pp. 80-84

Capacity of Diffusion-based Molecular Communication with Ligand Receptors

A. Einolghozati, M. Sardari and F. Fekri
pp. 85-89

Mutation and Optimal Search of Sequences in Nested Hamming Spaces

R. Belavkin
pp. 90-94

Voice Pathology Detection with Predictable Component Analysis and Wavelet Decomposition Model

P. Scalassara, L. Agnoletti dos Santos and C. Maciel
pp. 95-99

Lunch

S2A: Multi-terminal Information Theory I

A Strictly Improved Achievable Region for Multiple Descriptions Using Combinatorial Message Sharing

K. Viswanatha, E. Akyol and K. Rose
pp. 100-104

An Optimal Transmit-Receive Rate Tradeoff in Gray-Wyner Network and Its Relation to Common Information

K. Viswanatha, E. Akyol and K. Rose
pp. 105-109

A Lattice Compress-and-Forward Scheme

Y. Song and N. Devroye
pp. 110-114

Decode-forward and Compute-forward Coding Schemes for the Two-Way Relay Channel

P. Zhong and M. Vu
pp. 115-119

An achievable region for the double unicast problem based on a minimum cut analysis

S. Huang and A. Ramamoorthy
pp. 120-124

S2B: Coding for Wireless Systems

Optimal Rate for Irregular LDPC Codes in Binary Erasure Channel

H. Tavakoli
pp. 125-129

Reducing Complexity with Less than Minimum Delay Space-Time Lattice Codes

R. Vehkalahti and C. Hollanti
pp. 130-134

Diversity-multiplexing Gain Tradeoff: a Tool in Algebra?

R. Vehkalahti and H. f. Lu
pp. 135-139

Graph-based Codes for Quantize-Map-and-Forward Relaying

A. Sengupta, S. Brahma, A. Özgür, C. Fragouli and S. Diggavi
pp. 140-144

MAP decoding for LDPC codes over the Binary Erasure Channel

L. Salamanca, P. M. Olmos, J. J. Murillo-Fuentes and F. Pérez-Cruz
pp. 145-149

S2C: Sequences and Complexity

On Bent Functions Associated to AB Functions

L. Budaghyan, C. Carlet and T. Helleseeth
pp. 150-154

Quasi-Orthogonal Supersets

B. Popovic
pp. 155-159

Spectral Shaping Codes with Even Length Permutation Sequences

K. Ouahada
pp. 160-164

Ambiguity and Deficiency of Permutations from Finite Fields

D. Panario, A. Sakzad, B. Stevens and Q. Wang
pp. 165-169

Three-dimensional periodic Optical Orthogonal Code for OCDMA systems

J. Ortiz-Ubarri, O. Moreno and A. Tirkel
pp. 170-174

Coffee Break

S3A: Shannon Theory

Ultra-Small Block-Codes for Binary Discrete Memoryless Channels

C. Po-Ning, L. Hsuan-Yin and S. Moser
pp. 175-179

State-Dependent Channels with Composite State Information at the Encoder

A. Khina, M. Kesal and U. Erez
pp. 180-184

On the Capacity of Noisy Computations

F. Simon
pp. 185-189

Continuous-Time Directed Information and Its Role in Communication

H. Permuter, Y. H. Kim and T. Weissman
pp. 190-194

Capacity Bounds for Multiuser Channels with Non-Causal Channel State Information at the Transmitters

R. Khosravi-Farsani and F. Marvasti
pp. 195-199

Finite Block-Length Achievable Rates for Queuing Timing Channels

T. Riedl, T. Coleman and A. Singer
pp. 200-204

S3B: Codes, Lattices and Cryptography I

Information-Theoretic Analysis of Content Based Identification for Correlated Data

F. Farhadzadeh, S. Voloshynovskiy, O. Koval and F. Beekhof
pp. 205-209

On the Eavesdropper's Correct Decision in Gaussian and Fading Wiretap Channels Using Lattice Codes

A. M. Ernvall-Hytönen and C. Hollanti
pp. 210-214

A Lattice-Based Batch Identification Scheme

R. Silva, P. L. Cayrel and R. Lindner
pp. 215-219

Decoding q -ary lattices in the Lee metric

A. C. Campello, G. Jorge and S. Costa
pp. 220-224

Minimal codes in binary abelian group algebras

M. Guerreiro, R. Ferraz and C. Milies
pp. 225-228

List-Decoding of Binary Goppa Codes up to the Binary Johnson Bound

D. Augot, M. Barbier and A. Couvreur
pp. 229-233

S3C: Quantum Information Theory

Asymmetric quantum generalized Reed-Solomon codes

G. La Guardia
pp. 234-236

Robustness of Statistical Mechanical Interpretation of Algorithmic Information Theory

K. Tadaki
pp. 237-241

Helstrom's Theory on Quantum Binary Decision Revisited

G. Cariolaro and A. Vigato
pp. 242-246

Quantum Search Algorithms on Hierarchical Networks

F. Marquezino, R. Portugal and S. Boettcher
pp. 247-251

Quantum turbo codes with unbounded minimum distance and excellent error-reducing performance

M. Abbara and J. P. Tillich
pp. 252-256

Board Meeting

Tuesday, October 18

P2: Plenary Talk: Codes for distributed storage systems - Kannan Ramchandran

S4A: Graph-based Codes and Iterative Decoding

Iterative Soft Decoding of Binary Linear Codes Using a Generalized Tanner Graph

E. Rosnes
pp. 257-261

On-Line Fountain Codes for Semi-Random Loss Channels

Y. Cassuto and A. Shokrollahi
pp. 262-266

Multi-Edge Framework for Unequal Error Protecting LT Codes

H. Beltrão Neto, W. Henkel and V. da Rocha Jr.

pp. 267-271

Annotated Raptor Codes

K. Mahdavian, M. Ardakani and C. Tellambura

pp. 272-276

Universal Rateless Codes From Coupled LT Codes

V. Aref and R. Urbanke

pp. 277-281

S4B: Codes, Lattices and Cryptography II

A Distinguisher for High Rate McEliece Cryptosystems

J. C. Faugère, V. Gauthier, A. Otmani, L. Perret and J. P. Tillich

pp. 282-286

Information-Theoretically Secure Key-Insulated Key-Agreement

T. Seito and J. Shikata

pp. 287-291

LWE-based Identification Schemes

R. Silva, A. C. Campello and R. Dahab

pp. 292-296

Identification In Desynchronization Channels

O. Koval, S. Voloshynovskiy and F. Farhadzadeh

pp. 297-301

A tree construction method of nested cyclic codes

F. Barbosa and M. Costa

pp. 302-305

S4C: Communication Theory I

A Half-Duplex Relay Coding Scheme Optimized for Energy Efficiency

F. Parzysz, M. Vu and F. Gagnon

pp. 306-310

Amplify-and-Forward in Wireless Relay Networks

S. Agnihotri, S. Jaggi and M. Chen

pp. 311-315

An Information Theoretic Approach for Determining the Minimum Number of Sensors in a Wireless Sensor Network

B. Larish and G. Riley

pp. 316-320

Binary Arithmetic Coding for Time-Varying Sources Based on the Maskit Boundary

L. Leskow and R. Palazzo

pp. 321-324

Optimal HDA Codes for Sending a Gaussian Source over a Gaussian Channel with Bandwidth Compression

M. Varasteh and H. Behroozi
pp. 325-329

Coffee Break

S5A: Coding Theory and Practice II

Operating LDPC Codes with Zero Shaping Gap

G. Böcherer and R. Mathar
pp. 330-334

Multi-Edge Type Unequal Error Protecting Low-Density Parity-Check Codes

H. Beltrão Neto, W. Henkel and V. da Rocha Jr.
pp. 335-339

Ensemble Analysis of Pseudocodewords of Protograph-Based Non-Binary LDPC Codes

D. Divsalar and L. Dolecek
pp. 340-344

On the Selection of Finite Alphabet iterative decoders for LDPC codes on the BSC

L. Danjean, D. Declercq, S. Planjery and B. Vasić
pp. 345-349

Quasi-Cyclic LDPC Codes Based on Pre-Lifted Protographs

D. Mitchell, R. Smarandache and D. Costello
pp. 350-354

S5B: Communication Theory II

Precoding for Coded Communication on Block Fading Channels and Cooperative Communications

D. Duyck, J. J. Boutros and M. Moeneclaey
pp. 355-359

High SNR Bounds for the BICM Capacity

A. Alvarado, F. Brännström and E. Agrell
pp. 360-364

Communications Overhead as the Cost of Constraints

J. N. Laneman and B. Dunn
pp. 365-369

Equivalent Models for Multi-terminal Channels

F. Calmon, M. Médard and M. Effros
pp. 370-374

A Maximum Entropy Theorem for Complex-Valued Random Vectors, with Implications on Capacity

G. Tauböck
pp. 375-379

S5C: Signal Processing

Subspace based Multi-Dimensional Model Order Selection in Colored Noise Scenarios

J. P. da Costa, F. Roemer, D. Schulz and R. de Sousa Junior
pp. 380-384

Sign-Magnitude Decomposition of Mutual Information with Polarization Effect in Digital Identification

S. Voloshynovskiy, T. Holotyak, O. Koval, F. Beekhof and F. Farhadzadeh
pp. 385-389

Widely Linear SIMO Filtering for Hypercomplex Numbers

D. Schulz, J. Seitz and J. P. da Costa
pp. 390-394

Towards An Optimal Beamforming Algorithm for Physical Layer Multicasting

M. Khojastepour, A. Salehi-Golsefidi and S. Rangarajan
pp. 395-399

Incremental Coding over MIMO Channels

A. Khina, Y. Kochman, U. Erez and G. Wornell
pp. 400-404

Lunch

Excursion

Wednesday, October 19

P3: Plenary Talk: Jet list decoding - Daniel J. Bernstein

I2A: Invited Session III: Codes, Lattices and Cryptography

Organizer: Paulo Barreto

Algebraic solvers for certain lattice-related problems

J. Ding
pp. 405-409

Search to Decision Reduction for the Learning with Errors over Rings Problem

V. Lyubashevsky
pp. 410-414

The Tightness of Security Reductions in Code-based Cryptography

N. Sendrier

pp. 415-419

I2B: Invited Session IV: Multi-Terminal Information Theory

Organizer: Suhas Diggavi

Quantized Compute and Forward: A Low-Complexity Architecture for Distributed Antenna Systems

S. Hong and G. Caire

pp. 420-424

A Converse for the Wideband Relay Channel with Physically Degraded Broadcast

N. Fawaz and M. Médard

pp. 425-429

On Message Lengths for Noisy Network Coding

G. Kramer and J. Hou

pp. 430-431

Coffee Break

S6A: Multi-terminal Information Theory II

Capacity Bounds for the Z Channel

H. Do, T. Oechtering and M. Skoglund

pp. 432-436

Communicating Degraded Message Sets over Multi-access Channels with Degraded Encoder State Information

B. Vellambi and I. Land

pp. 437-441

Interference Alignment at Finite SNR for Time-Invariant Channels

Or Ordentlich and U. Erez

pp. 442-446

Feasibility of interference alignment for the MIMO interference channel: the symmetric square case

G. Bresler, D. Cartwright and D. Tse

pp. 447-451

On the capacity of multiplicative multiple access channels with AWGN

S. R. B Pillai

pp. 452-456

S6B: Source Coding

Fixed-length lossy compression in the finite blocklength regime: Gaussian source

V. Kostina and S. Verdú
pp. 457-461

Lossy Source Coding with Byzantine Adversaries

E. Ahmed and A. Wagner
pp. 462-466

Coordination using Implicit Communication

P. Cuff and L. Zhao
pp. 467-471

Achievability of Maximum Decoding Rate on Sequential Coding

M. Nishiara
pp. 472-475

On the Network-Wide Gain of Memory-Assisted Source Coding

M. Sardari, A. Beirami and F. Fekri
pp. 476-480

S6C: Coding Theory and Practice III

Kite Codes over Groups

X. Ma, S. Zhao, K. Zhang and B. M. Bai
pp. 481-485

A standard form for generator matrices with respect to the Niederreiter-Rosenbloom-Tsfasman metric

M. Alves
pp. 486-489

MacWilliams-type identity in Poset-Block spaces

J. Pinheiro and M. Firer
pp. 490-494

Zero-error codes for the noisy-typewriter channel

F. Ruiz and F. Pérez-Cruz
pp. 495-497

Binary Error Correcting Network Codes

Q. Wang, S. Jaggi and S. Y. Li
pp. 498-502

Lunch

S7A: Coding Theory and Practice IV

XOR's, Lower Bounds and MDS Codes for Storage

J. Plank
pp. 503-507

A Knuth-Based RDS-Minimizing Multi-Mode Code

C. Heymann, H. Ferreira and J. Weber
pp. 508-512

Rate-Compatible LDPC Convolutional Codes for Capacity-Approaching Hybrid ARQ

Z. Si, M. Andersson, R. Thobaben and M. Skoglund
pp. 513-517

Gigabit Rate Low-Power LDPC Decoder

E. Pisek, D. Rajan and J. Cleveland
pp. 518-522

S7B: Network Coding

On network coding for acyclic networks with delays

K. Prasad and B. S. Rajan
pp. 523-527

On the Optimal Block Length for Joint Channel and Network Coding

C. Koller, M. Haenggi, J. Kliewer and D. Costello
pp. 528-532

Optimality of Network Coding with Buffers

B. Haeupler, M. Kim and M. Médard
pp. 533-537

Exact Modeling of the Performance of Random Linear Network Coding in Finite-buffer Networks

N. Torabkhani, B. Vellambi, A. Beirami and F. Fekri
pp. 538-542

Full-Diversity Network Coding For Two-User Cooperative Communications

J. L. Rebelatto, B. Uchôa-Filho and D. Silva
pp. 543-547

S7C: Compressed Sensing

A Compressed Sensing Wire-Tap Channel

G. Reeves, N. Goela, N. Milosavljevic and M. Gastpar
pp. 548-552

Analysis of MMSE Estimation for Compressive Sensing of Block Sparse Signals

M. Vehkaperä, S. Chatterjee and M. Skoglund
pp. 553-557

Covering Radius and the Restricted Isometry Property

R. Calderbank, S. Jafarpour and M. Nastasescu
pp. 558-562

Secrecy using Compressive Sensing

S. Agrawal and S. Vishwanath
pp. 563-567

Critical Compression Ratio of Iterative Reweighted l_1 Minimization for Compressed Sensing

R. Matsushita and T. Tanaka
pp. 568-572

Coffee Break

S8A: Network Information Theory

A Generalized Network Alignment for Three-Source Three-Destination Multiple Unicast Networks with Delays

A. Ganesan, T. Bavarisetti, K. Prasad and B. S. Rajan
pp. 573-577

Relay-Assisted Multiple Access with Multi-Packet Reception Capability and Simultaneous Transmission and Reception

N. Pappas, A. Ephremides and A. Traganitis
pp. 578-582

Error Propagation and the Achievable Throughput-Delay Trade-off in Wireless Networks

R. Subramanian, I. Land, B. Vellambi and L. K. Rasmussen
pp. 583-587

On the Sum Capacity of Multiaccess Block-Fading Channels with Individual Side Information

Y. Deshpande, S. R. B Pillai and B. Dey
pp. 588-592

Unchaining from the Channel: Cooperative Computation over Multiple-access Channels

M. Nokleby and B. Aazhang
pp. 593-597

Optimal Utilization of a Cognitive Shared Channel with a Rechargeable Primary Source Node

N. Pappas, J. Jeon, A. Ephremides and A. Traganitis
pp. 598-602

S8B: Information Theory and Statistics

Threshold Effects in Parameter Estimation as Phase Transitions in Statistical Physics

N. Merhav
pp. 603-607

Sufficient Conditions for the Convergence of the Shannon Differential Entropy

J. Silva and P. Parada
pp. 608-612

Necessary and Sufficient Conditions for Zero-Rate Density Estimation

J. Silva and M. Derpich
pp. 613-617

An Immune-Inspired Information-Theoretic Approach to the Problem of ICA over a Galois Field

D. Silva, R. Attux, E. Nadalin, L. Duarte and R. Suyama
pp. 618-622

On the generalization of decode-and-forward and compress-and-forward for Gaussian relay channels

K. Luo, R. Gohary and H. Yanikomeroglu
pp. 623-627

Multiple Access Channel with Correlated Channel States and Cooperating Encoders

M. Zamanighomi, M. J. Emadi, F. Shirani Chaharsooghi and M. R. Aref
pp. 628-632

S8C: Cryptography and Data Security

2-Dimensional Interval Algorithm

T. Chan and S. W. Ho
pp. 633-637

Efficient Fully Simulatable Oblivious Transfer from the McEliece Assumptions

B. David and A. Nascimento
pp. 638-642

Enumerative encoding of correlation immune Boolean functions

N. Carrasco, J. M. Le Bars and A. Viola
pp. 643-647

A new Zero-knowledge code based identification scheme with reduced communication

C. Aguilar, P. Gaborit and J. Schrek
pp. 648-652

On the Separation of Encryption and Compression in Secure Distributed Source Coding

S. W. Ho, L. Lai and A. Grant
pp. 653-657

Key Agreement in State-dependent Channels with Non-causal Side Information

A. Zibaeenejad
pp. 658-662

Banquet

Thursday, October 20

I3A: Invited Session V: Graph-Based Codes and Iterative Decoding

Organizer: Daniel Costello

Existence and Uniqueness of GEXIT Curves via the Wasserstein Metric

S. Kudekar, T. Richardson and R. Urbanke
pp. 663-667

Coupled LDPC Codes: Complexity Aspects of Threshold Saturation

M. Lentmaier and G. Fettweis
pp. 668-672

The many applications of spatially-coupled codes

K. Kasai

I3B: Invited Session VI: Physical-layer Security

Organizer: Matthieu Bloch

Percolation in the Secrecy Graph: Bounds on the Critical Probability and Impact of Power Constraints

A. Sarkar and M. Haenggi
pp. 673-677

Hybrid Digital/Analog Schemes for Secure Transmission with Side Information

J. Villard, P. Piantanida and S. Shamai
pp. 678-682

A Cryptographic Treatment of the Wiretap Channel

M. Bellare, S. Tessaro and A. Vardy

S9A: Coding Theory and Practice V

A Note on Non-Binary Multiple Insertion/Deletion Correcting Codes

F. Palunčić, T. Swart, J. Weber, H. Ferreira and W. Clarke
pp. 683-687

Extended Bit-Flipping Algorithm for Solving Sparse Linear Systems of Equations Modulo p

A. Abolpour, M. R. Sadeghi and D. Panario
pp. 688-692

New Cyclically Permutable Codes

V. da Rocha Jr. and J. Lemos-Neto
pp. 693-697

S9B: Multi-terminal Information Theory III

Generating Dependent Random Variables Over Networks

A. Gohari and V. Anantharam
pp. 698-702

Towards the Capacity Region of Multiplicative Linear Operator Broadcast Channels

Y. Pang and T. Honold
pp. 703-707

Completion Time in Multi-Access Channel: An Information Theoretic Perspective

Y. Liu and E. Erkip
pp. 708-712

S9C: Physical-layer Security II

Bidirectional Broadcast Channels with Common and Confidential Messages

R. Wyrembelski and H. Boche
pp. 713-717

Secrecy Gain of Gaussian Wiretap Codes from Unimodular Lattices

F. Lin and F. Oggier
pp. 718-722

Linear Perfect Secret Key Agreement

C. Chan
pp. 723-726

Coffee Break

Panel: New Perspectives for Information Theory

Chair: Sergio Verdú